Deutscher Bundestag **Drucksache 17/8999**

17. Wahlperiode 15. 03. 2012

Fünfter Zwischenbericht

der Enquete-Kommission „Internet und digitale Gesellschaft“*

Datenschutz, Persönlichkeitsrechte

* Eingesetzt durch Beschluss des Deutschen Bundestages vom 4. März 2010 (Bundestagsdrucksache 17/950).

Inhaltsverzeichnis

Seite

Seite

Seite

Vorwort

Datenschutz betrifft uns alle. Insbesondere dann, wenn wir im Internet unterwegs sind. Denn hier werden viel größere Mengen an personenbezogenen Daten verarbeitet als in der analogen Welt. Das Leben im Internet mit immensem Datenfluss und sozialen Netzwerken stellt uns vor besondere Herausforderungen.

Aus diesem Grunde wurde in der Enquete-Kommission Internet und digitale Gesellschaft die Projektgruppe Datenschutz, Persönlichkeitsrechte eingesetzt. Seit ihrer Konstituierung am 14. Juni 2010 hat sich die Projektgruppe in 18 Sitzungen mit Fragen des Datenschutzes und der Persönlichkeitsrechte im Internet auseinandergesetzt.

Wir haben in der Projektgruppe neue Beteiligungsmöglichkeiten der Bürgerinnen und Bürger ausprobiert. Den so genannten 18. Sachverständigen – die Netzgemeinde – haben wir um Meinungen und Beteiligung gebeten. Wichtige Fragen haben wir auf der Microsite der Enquete-Kommission an die Öffentlichkeit gerichtet. Auch mit der Bürgerbeteiligungsplattform enquetebeteiligung.de beziehungsweise demokratie.de konnten wir neue Impulse und Anregungen erhalten. Wir haben für eine praktikable Bürgerbeteiligung viel ausprobiert. Und viel gelernt.

In einer Bestandsaufnahme haben wir im ersten Kapitel des Berichts einschlägige Regelungen und Rechtsprechung zusammengestellt. Im zweiten Kapitel wurden Problembereiche des Datenschutzes im Internet ausgemacht und beschrieben. Am Ende haben wir im dritten Kapitel Handlungsempfehlungen an den Bundestag formuliert.

Bedeutsames Gut beim Datenschutz des einzelnen Bürgers ist das Recht auf informationelle Selbstbestimmung. Das allgemeine Persönlichkeitsrecht ist für viele Fragen des Datenschutzes relevant. Wir haben auch widerstreitende Interessen erkannt und versucht, sie mit dem Datenschutz in Einklang zu bringen. Datenschutz ist nicht nur eine rechtliche Herausforderung, sondern eine gesamtgesellschaftliche Aufgabe. Fragen der Anonymität und der Umgang mit den eigenen Identitäten im Internet hängen auch von technischen Fragen, der Gestaltung von Diensten, aber auch gesellschaftlichen Normen ab.

Wichtig ist es auch, wie genau die Datennutzung durch die verantwortlichen Stellen erfolgt. Der Ausgleich zwischen Nutzerrechten und berechtigten Interessen von Anbietern und Betreibern ist möglich, aber noch längst nicht erreicht. Es kommt auch auf das Verhalten des Nutzers selbst an: Er kann und sollte sich mit Datenschutz auseinandersetzen, um möglichst informiert und frei entscheiden zu können, wie er mit seinen Daten umgehen will.

Nach intensiver Diskussion und Arbeit an den Texten haben wir im gemeinsamen Einvernehmen eine beachtliche Anzahl an Handlungsempfehlungen beschlossen. Für die intensive Zusammenarbeit möchte ich mich als Vorsitzender der Projektgruppe bei den Beteiligten bedanken. Ich sehe den Datenschutz – allen vereinzelt zu vernehmenden Unkenrufen zum Trotz – auf einem guten Weg. Es muss nicht alles neu erfunden werden, wenngleich Überarbeitungen sinnvoll und notwendig sind. Die Arbeit in der Projektgruppe Datenschutz mit den Kollegen und Sachverständigen hat mir Freude bereitet.

Manuel Höferlin
Vorsitzender der Projektgruppe Datenschutz, Persönlichkeitsrechte

1 Bestandsaufnahme bestehender Datenschutzregelungen[1]

1.1 Völkerrecht

1.1.1 Allgemeine völkerrechtliche Abkommen zum Schutz der Menschenrechte

Die frühen allgemeinen Menschenrechtsabkommen enthalten kein eigenes Datenschutzgrundrecht. Dennoch erstreckt sich der Schutzbereich dieser Abkommen auf den Datenschutz, und zwar im Rahmen des Schutzes des Privatlebens und des Schriftverkehrs.

So hat nach Artikel 8 der Europäischen Menschenrechtskonvention[2] (EMRK) „jede Person […] das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“. Der Schutz des Privatlebens umfasst auch den Schutz persönlicher, insbesondere medizinischer oder sozialer Daten.[3] Als Korrespondenz im Sinne von Artikel 8 EMRK gelten auch die Individualkommunikation mittels E-Mail, Telefon und Internettelefonie.[4] Staatliche Eingriffe sind nur auf gesetzlicher Grundlage unter den in der Vorschrift genannten Voraussetzungen zulässig, zum Beispiel zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Die Regelung stellt nicht nur ein Abwehrrecht gegen staatliche Eingriffe dar, sie begründet auch staatliche Schutz- und Handlungspflichten, etwa zum Erlass entsprechender Regelungen.[5] Nach Artikel 1 EMRK sichern die Vertragsparteien dieses völkerrechtlichen Vertrages allen ihrer Hoheitsgewalt unterstehenden Personen unter anderem die in Artikel 8 EMRK bestimmten Rechte und Freiheiten zu. In Deutschland stellt Artikel 8 EMRK unmittelbar geltendes Recht dar.

In ähnlicher Weise bestimmt Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte (IPBürgR)[6], dass „niemand […] willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden“ darf. „Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“ Wie bei der EMRK ist auch bei diesem Menschenrechtsabkommen der Vereinten Nationen der Datenschutz ein Element der Privatsphäre. Die Regelung gilt sowohl hinsichtlich staatlicher Eingriffe, als auch bei Eingriffen Privater. Die Vertragsstaaten, darunter die Bundesrepublik Deutschland, sind verpflichtet, Rechtsschutz gegenüber staatlichen Eingriffen zu ermöglichen und Regelungen zum Schutz vor privaten Eingriffen zu treffen.[7]

Artikel 16 der so genannten Kinderrechtskonvention[8] deckt sich im Wortlaut mit Artikel 17 IPBürgR. Träger der gewährten Rechte ist nach Artikel 16 des Kinderrechte-Übereinkommens jedoch ausdrücklich das Kind.

Da bei den vorgenannten Menschenrechtsabkommen der Datenschutz lediglich als Teil des Schutzes des Privatlebens anzusehen und daher nur sehr allgemein ausgeprägt ist, ergeben sich datenschutzspezifische Details allenfalls aus Einzelfallentscheidungen der jeweils zuständigen Instanzen. Allerdings enthält gerade die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) zu Artikel 8 EMRK zahlreiche Hinweise auf den Schutzbereich des Datenschutzes und entsprechende Eingriffsvoraussetzungen.

In dem jüngeren Übereinkommen der Vereinten Nationen über die Rechte von Menschen mit Behinderungen (Behindertenrechtskonvention – BRK)[9] werden in Artikel 22 („Achtung der Privatsphäre“), der in seinem sonstigen Wortlaut weitgehend Artikel 17 IPBürgR entspricht, Fragen der informationellen Selbstbestimmung und des Datenschutzes ausdrücklich thematisiert. So sind neben dem Schriftverkehr ausdrücklich auch „andere Arten der Kommunikation“ vor willkürlichen und rechtswidrigen Eingriffen geschützt. Außerdem erklären die Vertragsstaaten, „auf der Grundlage der Gleichberechtigung mit anderen die Vertraulichkeit von Informationen über die Person, die Gesundheit und die Rehabilitation von Menschen mit Behinderungen“ zu schützen.

1.1.2 Datenschutz in völkerrechtlichen Spezialregelungen

Die Leitlinien der OECD für den Schutz des Persönlichkeitsrechts und den grenzüberschreitenden Verkehr personenbezogener Daten[10], bei denen es sich nicht um einen völkerrechtlichen Vertrag, sondern um eine Empfehlung an die Mitgliedstaaten der Organisation handelt, stellen einen frühen Versuch dar, Datenschutz, freien Informationsfluss und freien Handelsverkehr in Ausgleich zu bringen. Da neben EU-Mitgliedstaaten unter anderem die USA Mitglied der OECD sind, waren hierbei europäische und US-amerikanische Ansätze des Datenschutzes zu berücksichtigen.[11] In den Leitlinien wird zwischen „sensiti-

1 Stand des Kapitels 1: 7. März 2011.

2 Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, BGBl. II 1952, S. 686.

3 Vgl. Meyer-Ladewig, Jens: EMRK, Handkommentar. 3. Auflage 2011, Artikel 8 EMRK Rn. 40.

4 Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 37.

5 Vgl. Meyer-Ladewig, Jens: EMRK, Handkommentar. 3. Auflage 2011, Artikel 8 EMRK Rn. 2.

6 Internationaler Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966, BGBl. II 1973, S. 1533.

7 Vgl. Hofmann, Rainer/Boldt, Nicki: Kommentar zu dem Internationalen Pakt über bürgerliche und poltische Rechte, in: Kölble, Josef (Hrsg.). Das Deutsche Bundesrecht – Systematische Sammlung der Gesetze und Verordnungen mit Erläuterungen. Hauptband 1949, Erl. zu Artikel 17 IPbpR.

8 Übereinkommen der Vereinten Nationen über die Rechte des Kindes vom 20. November 1989, BGBl. II 1992, S. 122.

9 Übereinkommen über die Rechte von Menschen mit Behinderungen vom 13. Dezember 2006, BGBl. II 2008, S. 1419.

10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data vom 23. September 1980, Bundesanzeiger Nr. 251 vom 14. November 1981.

11 Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 36.

ven“ und „trivialen“ Angaben[12], von denen offensichtlich keine Gefahr ausgeht, unterschieden. Letztere können von der Anwendung der Leitlinien ausgeschlossen werden. Neben verschiedenen Verarbeitungsgrundsätzen für den innerstaatlichen Bereich enthalten die Leitlinien Empfehlungen zur Sicherung des freien Informationsflusses zwischen den Mitgliedstaaten. So soll etwa auf unangemessen hohe Datenschutzregelungen, die den grenzüberschreitenden Datenverkehr behindern, verzichtet werden. Der Selbstregulierung wird gleicher Stellenwert wie der (nationalen) Gesetzgebung eingeräumt.[13] Die Leitlinien gelten als „Indiz für die internationale Verbreitung bestimmter Datenschutzgrundsätze“[14], die jedoch weder völkerrechtliche Verbindlichkeit noch einen hohen Schutzstandard aufweisen. Dessen ungeachtet sollen sie jedoch auch dazu beigetragen haben, „den Datenschutz als Gegenstand internationaler Regulierung zu etablieren.“[15]

Die Europäische Datenschutzkonvention des Europarates[16] begründet hingegen rechtliche Verpflichtungen der Unterzeichnerstaaten, einen bestimmten Katalog von Datenschutzgrundsätzen einzuhalten und in nationales Recht umzusetzen.[17] Dazu gehört insbesondere die Einhaltung bestimmter Verarbeitungsgrundsätze nach Artikel 5 des Übereinkommens, die zugleich einen Kanon der heute noch gültigen Grundregeln des Datenschutzes darstellen. Personenbezogene Daten, die im öffentlichen oder nicht-öffentlichen Bereich automatisch verarbeitet werden, müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft und verarbeitet werden. Die Speicherung und Verwendung ist nur für festgelegte, rechtmäßige Zwecke zulässig. Die Daten müssen im Sinne des Verhältnismäßigkeitsgrundsatzes diesen Zwecken entsprechen und dürfen nicht darüber hinaus gehen. Die sachliche Richtigkeit der Daten, gegebenenfalls durch spätere Aktualisierung, ist genauso vorgeschrieben wie die Anonymisierung der Daten nach Zweckerfüllung. Das Übereinkommen sieht weiterhin ein spezifisches Schutzniveau für besonders sensible Daten (etwa über politische Anschauungen oder Gesundheitsdaten) und bestimmte Rechte der Betroffenen vor. Nach Artikel 1 des Zusatzprotokolls „betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr“ vom 8. November 2001[18] sind unabhängige Kontrollstellen einzurichten, die insbesondere die Einhaltung der in nationales Recht umgesetzten Grundsätze für den Datenschutz gewährleisten sollen. Sie nehmen ihre Aufgaben „in völliger Unabhängigkeit“ wahr. Das Zusatzprotokoll beschränkt weiterhin in Artikel 2 die Datenübermittlung in Staaten, die nicht Mitglied des Übereinkommens sind. Sie ist nur dann zulässig, wenn im Empfängerstaat ein „angemessenes Schutzniveau“ gewährleistet ist. Die Weitergabe der Daten kann aber beispielsweise auch dann erlaubt werden, wenn vertragliche Garantien von der zuständigen Behörde für ausreichend befunden wurden.

Die Cybercrime Convention des Europarates vom 23. November 2001[19] enthält strafrechtliche Mindeststandards im Falle von Angriffen auf Computer- und Telekommunikationssysteme sowie ihrem Missbrauch zur Begehung von Straftaten, Vorgaben zu strafprozessualen Maßnahmen, zur Durchsuchung und Beschlagnahme bei solchen Straftaten und Regelungen zur Verbesserung der internationalen Zusammenarbeit einschließlich der Rechtshilfe bei deren Verfolgung.[20]

Als datenschutzrechtliche Spezialregelung mit globalem Anwendungsbereich kann der Beschluss der Generalversammlung der Vereinten Nationen vom 14. Dezember 1990 über „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien“ gelten.[21] Diese Richtlinien, die jedoch ein niedrigeres Datenschutzniveau aufweisen als die oben genannten Abkommen, haben lediglich den Charakter einer Empfehlung.

1.2 Europarecht

1.2.1 Europäisches Primärrecht

Durch das Inkrafttreten des Vertrags von Lissabon hat der Datenschutz auf EU-Ebene eine Stärkung erfahren und ist nun an zwei Stellen ausdrücklich im Primärrecht verankert:

Die grundsätzliche Regelung findet sich im Vertrag über die Arbeitsweise der Europäischen Union (AEUV). Sie ist mit Artikel 16 AEUV an herausgehobener Stelle im Titel II (Allgemein geltende Bestimmungen) verortet und soll so gewährleisten, dass der Datenschutz bei sämtlichen in den EU-Verträgen erfassten Bereichen und Politiken gilt.[22] Artikel 16 AEUV [Datenschutz] lautet:

---

[12] Vgl. Simitis, Spiros, in: ders. (Hrsg.). Bundesdatenschutzgesetz. 6. Auflage 2006, Einleitung Rn. 186.

[13] Vgl. Simitis, Spiros, in: ders. (Hrsg.). Bundesdatenschutzgesetz. 6. Auflage 2006, Einleitung Rn. 198.

[14] Ennulat, Mark: Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und -einrichtungen. 2008, S. 72.

[15] Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 36.

[16] Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981, BGBl. II 1985, S. 538.

[17] Nach Nr. 39 der Denkschrift zum Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten, Bundestagsdrucksache 16/7218, S. 40, können die zur Umsetzung zu ergreifenden Maßnahmen neben Gesetzen verschiedene Formen annehmen, wie Verordnungen usw. Bindende Maßnahmen können durch freiwillige Regelungen „ergänzt“ werden, die jedoch allein nicht ausreichend sind.

[18] Zusatzprotokoll zu dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 8. November 2001, BGBl. II 2002, S. 1882.

[19] Übereinkommen über Computerkriminalität des Europarates vom 23. November 2001, BGBl. II 2008, S. 1242; für die Bundesrepublik Deutschland in Kraft getreten mit Wirkung vom 1. Juli 2009.

[20] Vgl. Denkschrift zu dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (I. Allgemeines), Bundestagsdrucksache 16/7218, S. 40.

[21] Guidelines on the Use of Computerized Personal Data Flow, Resolution der Generalversammlung vom 14. Dezember 1990, UN Doc. A/Res/45/95.

[22] Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Auflage 2010, Artikel 16 AEUV Rn. 7.

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.[…]“

Artikel 16 AEUV enthält in Absatz 1 erstmals ein primärrechtliches Grundrecht des Datenschutzes[23], das sowohl gegenüber den Organen, Einrichtungen und sonstigen Stellen der EU gilt als auch gegenüber den Mitgliedstaaten, soweit sie im Anwendungsbereich des Unionsrechts handeln. Korrespondierend zu diesem Rechtsanspruch auf Datenschutz ist in Absatz 2 erstmals auf primärrechtlicher Ebene eine einzige und allgemeine Rechtsetzungsbefugnis der EU ausschließlich zum Schutz personenbezogener Daten normiert. So werden das Europäische Parlament und der Rat der EU im Bereich des Datenschutzes ermächtigt, Gesetzgebungsakte nach dem ordentlichen Gesetzgebungsverfahren zu beschließen.[24]

Daneben wurde mit dem Vertrag von Lissabon durch Artikel 39 des Vertrags über die Europäische Union (EUV) eine Beschlussvorschrift zum Datenschutz speziell für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik eingeführt. Artikel 39 EUV („Schutz personenbezogener Daten“) lautet:

„Gemäß Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und abweichend von Absatz 2 des genannten Artikels erlässt der Rat einen Beschluss zur Festlegung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich dieses Kapitels fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.“

Artikel 39 EUV knüpft an die allgemeine Vorschrift des Artikel 16 AEUV an, verlangt aber für die nähere Regelung des Datenschutzes im Bereich der Gemeinsamen Außen- und Sicherheitspolitik ein anderes Verfahren der Rechtsetzung, und zwar einen Beschluss des Rates.[25]

Mit dem Vertrag von Lissabon wurde schließlich die Charta der Grundrechte der Europäischen Union[26] (GRC) im Dezember 2009 rechtsverbindlich. Sie steht nun auf gleicher Hierarchiestufe wie das Primärrecht.[27] Die Vorschrift des Artikel 8 GRC, die parallel zu Artikel 16 AEUV den Schutz personenbezogener Daten regelt, stimmt in ihrem Absatz 1 wörtlich mit Artikel 16 Absatz 1 AEUV überein; Absatz 2 formt das unionale Grundrecht näher aus.[28] Artikel 8 GRC („Schutz personenbezogener Daten“) lautet:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

Das Grundrecht auf Datenschutz gemäß Artikel 8 GRC verpflichtet nach Artikel 51 Absatz 1 Satz 1 GRC zunächst die Organe und Einrichtungen der EU bei sämtlichen ihrer Aktivitäten; es gibt keinen grundrechtsfreien Raum in der EU.[29] Darüber hinaus sind auch die Mitgliedstaaten auf das unionale Grundrecht auf Datenschutz „bei der Durchführung des Rechts der Union“ gemäß Artikel 51 Absatz 1 Satz 1 GRC verpflichtet.[30] Eine Bindung der Mitgliedstaaten an das unionale Grundrecht des Datenschutzes ist damit in jedem Fall bei der legislativen Umsetzung von Richtlinien und beim administrativen Vollzug von Verordnungen oder unmittelbar anwendbaren Richtlinien durch die Mitgliedstaaten gegeben.[31] Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) sind die Grundrechte der Union von den Mitgliedstaaten jedoch über die bloße Durchführung des

[23] Vgl. Kotzur, Markus, in: Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV. 5. Auflage 2010, Artikel 16 AEUV Rn. 2; Kingreen, Thorsten, in: Calliess, Christian/Ruffert, Matthias (Hrsg.). EUV/EGV - Das Verfassungsrecht der Europäischen Union. 3. Auflage 2007, Artikel 286 EGV Rn. 29; Hatje, Armin, in: Schwarze, Jürgen (Hrsg.). EU-Kommentar. 2. Auflage 2009, Artikel 286 EGV Rn. 6.

[24] Im Zusammenhang mit Artikel 16 AEUV sind weiterhin die „Erklärung Nr. 20 zu Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union“ und die „Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit“ relevant, beides veröffentlicht in: Rat der Europäischen Union, Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, Dok.-Nr. 6655/08, vom 15. April. 2008.

[25] Vgl. Geiger, Rudolf, in: ders./Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV, 5. Auflage 2010, Artikel 39 EUV Rn. 3.

[26] ABl. EU Nr. C 83 vom 30. März 2010, S. 393, in Kraft getreten am 1. Dezember 2009.

[27] Siehe Artikel 6 Absatz 1 EUV.

[28] Vgl. Kotzur, Markus, in: Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV. 5. Auflage 2010, Artikel 16 AEUV Rn. 2; Hatje, Armin, in: Schwarze, Jürgen (Hrsg.). EU-Kommentar. 2. Auflage 2009, Artikel 286 EGV Rn. 6.

[29] Vgl. Jarass, Hans D.: Charta der Grundrechte der Europäischen Union. 2010, Artikel 51 Rn. 4.

[30] Vgl. hierzu Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System. 2009, S. 396 ff.

[31] Vgl. Kingreen, Thorsten, in: Calliess, Christian/Ruffert, Matthias (Hrsg.). EUV/EGV – Das Verfassungsrecht der EU. 2007, Artikel 51 GRCh Rn. 8; Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System. 2009, S. 390.

Unionsrechts hinaus schon dann anzuwenden, wenn eine nationale Maßnahme in den Anwendungsbereich des Unionsrechts fällt, zum Beispiel in den Fällen, in denen die Mitgliedstaaten Grundfreiheiten des Binnenmarkts einschränken.[32] Überwiegend wird in der Rechtswissenschaft davon ausgegangen, dass diese weite Auslegung des EuGH durch das Verbindlichwerden der GRC nicht tangiert wird.[33] Festzuhalten bleibt, dass das unionale Grundrecht auf Datenschutz nur dann nicht in den Mitgliedstaaten zum Tragen kommt, wenn sie allein im Rahmen ihrer nationalen Kompetenzen agieren.[34]

1.2.2 Europäisches Sekundärrecht

Das zentrale Datenschutzinstrument auf europäischer Ebene ist die Datenschutzrichtlinie 95/46/EG[35] aus dem Jahr 1995 (DSRL). Die Richtlinie verpflichtet die Mitgliedstaaten, für die Verarbeitung personenbezogener Daten bestimmte Mindeststandards in ihre nationale Gesetzgebung zu übernehmen. Sie zielt darauf ab, den Schutz der Privatsphäre natürlicher Personen und den grundsätzlich erwünschten freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten in Einklang zu bringen. Deshalb sieht die Richtlinie auch vor, dass der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten nicht unter Hinweis auf den Schutz der Grundrechte und Grundfreiheiten, insbesondere des Schutzes der Privatsphäre, beschränkt oder untersagt werden darf. Die Mitgliedstaaten können also keine Datenschutzstandards einführen, die von den in der Richtlinie festgelegten Mindeststandards abweichen, wenn dadurch der freie Verkehr der Daten innerhalb der EU eingeschränkt wird. Die Datenschutzrichtlinie ist nicht anwendbar auf die Verarbeitung personenbezogener Daten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts vor dem Vertrag von Lissabon fallen. Hierunter fallen insbesondere Tätigkeiten der Europäischen Union in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (frühere dritte Säule). Eine Anpassung der Richtlinie an die mit dem Vertrag von Lissabon bewirkte Auflösung der Säulenstruktur ist bislang noch nicht erfolgt.[36]

Die in der Richtlinie vorgeschriebenen datenschutzrechtlichen Mindeststandards betreffen

- die Qualität der Daten (unter anderem Verarbeitung nach Treu und Glauben, auf rechtmäßige Weise sowie für festgelegte Zwecke),
- die Zulässigkeit der Datenverarbeitung (unter anderem bei Einwilligung der betroffenen Person oder Erforderlichkeit der Datenverarbeitung aus bestimmten in der Richtlinie festgelegten Gründen),
- erhöhte Schutzanforderungen für besonders sensible Daten, etwa betreffend die politische Meinung oder die religiöse Überzeugung;
- bestimmte Informationen, die der für die Verarbeitung Verantwortliche der betroffenen Person übermitteln muss,
- Auskunftsrechte sowie Rechte auf Berichtigung, Löschung und Sperrung von Daten,
- Widerspruchsrechte,
- die Vertraulichkeit und Sicherheit der Verarbeitung,
- Meldepflichten gegenüber einer Kontrollstelle,
- Rechtsbehelfe, Haftung und Sanktionen.

Die Richtlinie sieht weiterhin die Einrichtung von Kontrollstellen vor, die ihre Aufgaben in völliger Unabhängigkeit wahrnehmen und legt Grundsätze für die Übermittlung personenbezogener Daten an Drittstaaten fest. Voraussetzung hierfür ist, dass der Drittstaat ein „angemessenes Schutzniveau“[37] gewährleistet. Bei welchen Staaten dies der Fall ist, entscheidet die Kommission.

Der Verpflichtung zur Umsetzung der Richtlinie, die bis 1998 zu erfüllen war, ist Deutschland durch Änderung des Bundesdatenschutzgesetzes im Jahr 2001 nachgekommen.

Bei der Umsetzung der Vorschriften über die Datenübermittlung in Drittländer ergaben sich gegenüber den USA Probleme, die zum Abschluss der Safe-Harbor-Vereinbarung führten. Aufgrund unterschiedlicher datenschutzrechtlicher Ansätze verfolgen die USA in Fragen des Datenschutzes einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung beruht, während in der EU Regelungen in Form umfassender Datenschutzgesetze überwiegen. Angesichts dieser Unterschiede bestanden Unsicherheiten, ob bei der Übermittlung personenbezogener Daten in die USA ein angemessenes Schutzniveau im Sinne des EU-Datenschutzrechts gegeben sei.[38] Um ein angemessenes Datenschutzniveau zu gewährleisten, haben die EU

[32] EuGH, Urteil v. 18. Juni 1991, Rs. C-260/89, Slg. 1991, S. I-2925, Rn. 42 ff. = EuGRZ 1991, S. 274 – ERT (Leiturteil). Hierzu Scheuing, Dieter H.: Zur Grundrechtsbindung der EU-Mitgliedstaaten. EuR 2005, 162 (164); Kokott, Juliane/Sobotta, Christoph: Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon. EuGRZ 2010, 265 (268).

[33] Vgl. Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System. 2009, S. 398; Kokott, Juliane/Sobotta, Christoph: Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon. EuGRZ 2010, 265 (268).

[34] Vgl. Jarass, Hans D.: Charta der Grundrechte der Europäischen Union. 2010, Artikel 51 Rn. 10.

[35] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 vom 23. November 1995, S. 31. Im Folgenden „Datenschutzrichtlinie“.

[36] Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Auflage 2010, Artikel 16 AEUV Rn. 37.

[37] Artikel 25 DSRL.

[38] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, KOM (2000) 2441, ABl. EG Nr. L 215 vom 25. August 2000, S. 10.

und das US-Handelsministerium im Juli 2006 eine Vereinbarung zu den Grundsätzen des so genannten sicheren Hafens (Safe Harbor) geschlossen.[39] Als Safe-Harbor-Prinzipien wurden sieben Grundsätze für die Datenverarbeitung festgelegt (betreffend unter anderem Informationspflichten und Auskunftsrechte, Möglichkeit des Opt-out bei der Weitergabe an Dritte oder der Nutzung für andere Zwecke, Sicherheitsvorkehrungen gegen Verlust, unbefugten Zugriff oder Missbrauch personenbezogener Daten, Rechtsbehelfe und Sanktionen). Das Abkommen sieht vor, dass sich US-amerikanische Unternehmen öffentlich zur Einhaltung der Safe-Harbor-Prinzipien verpflichten können. Die Zertifizierung erfolgt durch Meldung an die Federal Trade Commission (FTC). Eine Liste der beigetretenen Unternehmen wird von der FTC im Internet veröffentlicht. Die Datenübermittlung an ein zertifiziertes Unternehmen ist dann möglich, ohne dass es einer weiteren behördlichen Feststellung des angemessenen Schutzniveaus bedürfte.[40]

Als bereichsspezifische Ergänzung der Datenschutzrichtlinie regelt die E-Privacy-Richtlinie 2002/58/EG[41] datenschutzrechtliche Aspekte im Bereich der elektronischen Kommunikation, die durch die Datenschutzrichtlinie nicht ausreichend abgedeckt wurden. Dies betrifft etwa die Vertraulichkeit der Kommunikation, Regelungen über Verkehrs- und Standortdaten, den Einzelgebührennachweis, die Rufnummernanzeige und unerbetene Werbenachrichten. Juristische Personen werden in den Schutzbereich der Richtlinie einbezogen. Die Richtlinie dient neben der Harmonisierung der mitgliedstaatlichen Datenschutzvorschriften auch der Gewährleistung des freien Verkehrs von Daten sowie elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft.

Die E-Privacy-Richtlinie wurde mit Richtlinie 2009/136/EG[42] geändert. Erstmalig wurde auf EU-Ebene eine Informationspflicht der Diensteanbieter bei Datensicherheitsverletzungen eingeführt, die Installation von Cookies oder Spyware von der Einwilligung der Internetnutzer abhängig gemacht, die Rechte Betroffener gegen unerbetene kommerzielle Nachrichten gestärkt und die Durchsetzung der Datenschutzbestimmungen durch Sanktionen verbessert.

In der im Jahr 2000 verabschiedeten E-Commerce-Richtlinie 2000/31/EG[43], mit der ein europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr geschaffen wurde, werden Fragen des Datenschutzes ausgeklammert[44] und insoweit auf anderweitige Rechtsakte der Union verwiesen. In den Erwägungen der Richtlinie (Nr. 14) wird allerdings betont, dass die Grundsätze des Schutzes personenbezogener Daten bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten sind, insbesondere in Bezug auf nicht angeforderte kommerzielle Kommunikation und die Verantwortlichkeit von Vermittlern.

Die Datenschutzverordnung für die EU-Organe 45/2001/EG[45] beschreibt den datenschutzrechtlichen Rahmen für das Handeln der EU-Organe. Adressat der Verordnung sind also nicht die Mitgliedstaaten, sondern alle „Organe und Einrichtungen der Gemeinschaft“. Durch die Verordnung wird weiterhin der Europäische Datenschutzbeauftragte eingesetzt, der für die unabhängige Kontrolle der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU zuständig ist.

Mit der Vorratsdatenspeicherungsrichtlinie 2006/24/EG[46] werden die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung bestimmter Daten, die von Telekommunikationsdienstleistern etwa im Rahmen von Internet und Telefonie erzeugt oder verarbeitet werden, harmonisiert. Auf diese Weise soll sichergestellt werden, dass die Daten zu Zwecken der Ermittlung und Verfolgung schwerer Straftaten verfügbar sind.[47] Die Richtlinie schreibt die vorsorgliche anlasslose Speicherung von Kommunikationsdaten vor und trifft unter anderem Feststellungen zu den Kategorien der zu speichernden Daten, zu Speicherungsfristen und Fragen des Datenschutzes und der Datensicherheit. Daten, die Kommunikationsinhalte betreffen (Inhaltsdaten), sind nicht zu speichern.[48]

---

[39] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000, ABl. EG Nr. L 215 vom 25. August 2000, S. 7.

[40] Nach einem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover sind die datenexportierenden Unternehmen in Deutschland dennoch verpflichtet, gewisse Mindestkriterien zu prüfen, da eine „flächendeckende“ Kontrolle durch die Kontrollbehörden, ob zertifizierte Unternehmen die Safe-Harbor-Prinzipien tatsächlich einhalten, nicht gegeben sei. Online abrufbar unter: http://www.bfdi.bund.de/cae/servlet/contentblob/1103868/publicationFile/88848/290410_SafeHarbor.pdf

[41] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 vom 31. Juli 2002, S. 37. Im Folgenden „E-Privacy-Richtlinie“.

[42] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. EU Nr. L 337 vom 18. Dezember 2009, S. 11.

[43] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), ABl. EG L 178 vom 17. Juli 2000, S. 1. Im Folgenden „E-Commerce-Richtlinie“.

[44] A. a. O. (S. 3), Erwägungsgrund Nr. 14, sowie Artikel 1 Absatz 5 b) der genannten Richtlinie.

[45] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft zum freien Datenverkehr, ABl. EG Nr. L 8 vom 12. Januar 2001, S. 1.

[46] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentliche zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105 vom 13. April 2006, S. 54. Im Folgenden „Vorratsdatenspeicherungsrichtlinie“.

[47] Artikel 1 Vorratsdatenspeicherungsrichtlinie, a. a. O.

[48] Zu den Entscheidungen des Bundesverfassungsgerichts, die die Umsetzung der Richtlinie in deutsches Recht betreffen, vgl. auch unter 1.3.4.

Im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS) existiert als allgemeiner Rechtsakt der Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.[49] Sein eng gefasster Anwendungsbereich erstreckt sich auf personenbezogene Daten, die von mitgliedstaatlichen Behörden zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen erhoben beziehungsweise verarbeitet werden. Der Beschluss gilt nur bei zwischenstaatlichem Datenaustausch und ist daher auf rein nationale Sachverhalte nicht anwendbar.[50] Im Gegensatz zur Datenschutzrichtlinie setzt der Rahmenbeschluss 2008/977/JI zwischen den Mitgliedstaaten lediglich einen Mindeststandard fest. Die einzelnen Mitgliedstaaten sind daher nicht gehindert, strengere nationale Bestimmungen im Regelungsbereich des Rahmenbeschlusses zu erlassen.[51]

Die Europäische Kommission hat im November 2010 ein Gesamtkonzept für den Datenschutz in der Europäischen Union[52] vorgelegt und einen Vorschlag für die Änderung der Datenschutzrichtlinie angekündigt.

1.2.3 Rechtsprechung des Europäischen Gerichtshofs

Erste Entscheidungen des EuGH zur Datenschutzrichtlinie datieren aus dem Jahr 2003.[53] In einem 2003 entschiedenen Verfahren[54] wandten sich Mitarbeiter des Österreichischen Rundfunks gegen eine österreichische Regelung, aufgrund derer ihre Jahresbezüge mit ihren Namen dem Rechnungshof mitzuteilen waren und nachfolgend vom Rechnungshof veröffentlicht wurden. Besonders streitig war in diesem Zusammenhang, ob die Datenschutzrichtlinie, die auf die Kompetenz der Gemeinschaft zur Errichtung des Binnenmarktes gestützt wurde und durch Harmonisierung der nationalen Vorschriften den freien Datenverkehr zwischen den Mitgliedstaaten gewährleisten sollte, auf diesen Sachverhalt überhaupt anwendbar war. Denn im konkreten Fall lag ein Zusammenhang mit den europarechtlichen Grundfreiheiten eher fern. Das Gericht hat die Anwendbarkeit der Richtlinie dennoch bejaht. Nach Auffassung des Gerichts kann die Anwendbarkeit der Richtlinie im Einzelfall nicht davon abhängen, ob ein Zusammenhang mit dem freien Verkehr zwischen den Mitgliedstaaten besteht.[55]

Die Darstellung anderer Personen ohne deren Zustimmung auf einer privaten schwedischen Webseite war Gegenstand im Fall Lindqvist[56]. In seinem Urteil nahm der EuGH erstmals zur Veröffentlichung personenbezogener Daten im Internet Stellung und entschied, dass die Einstellung ins Internet zwar eine Verarbeitung von Daten im Sinne der Datenschutzrichtlinie darstelle, nicht aber als Übermittlung in Drittländer und damit nicht als grenzüberschreitender Datenaustausch anzusehen sei. Das Gericht äußerte sich auch zur Frage des Ausgleichs zwischen Datenschutz und widerstreitenden Grundrechten, insbesondere der Meinungsfreiheit. Es sei Sache der nationalen Behörden und Gerichte, ein angemessenes Gleichgewicht zwischen den betroffenen Rechten und Interessen einschließlich geschützter Grundrechte herzustellen und hierbei insbesondere den Grundsatz der Verhältnismäßigkeit zu wahren. Im Übrigen sei es zulässig, dass die Mitgliedstaaten den Geltungsbereich ihrer Datenschutzgesetze über den Anwendungsbereich der Richtlinie hinaus ausdehnten, soweit dem keine Bestimmung des Gemeinschaftsrechts entgegenstehe.

Zur Übermittlung von Fluggastdaten an die USA nahm der EuGH im Mai 2006 Stellung.[57] Er erklärte die zugrunde liegende Genehmigung des Abkommens zwischen der EU und den USA durch den Rat für nichtig. Dasselbe gelte für die zum selben Sachverhalt ergangene Entscheidung der Kommission, mit der das US-amerikanische Datenschutzniveau für angemessen im Sinne des Artikel 25 DSRL erklärt wurde. Wie sich aus den Begründungserwägungen ergebe, seien Sinn und Zweck der Datenübermittlung in die USA die Terrorismusbekämpfung. Gegenstand beider Rechtsakte sei daher das Strafrecht. Daher sei die Datenschutzrichtlinie[58] keine geeignete Rechtsgrundlage. Mangels Rechtsgrundlage waren der Ratsbeschluss und die Kommissionsentscheidung deshalb für nichtig zu erklären.

In einem Urteil vom Februar 2009 über die Vorratsdatenspeicherungsrichtlinie[59] konzentriert sich der EuGH ebenfalls auf Fragen der Rechtsetzungskompetenz.

---

[49] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. EU Nr. L 350 vom 30. Dezember 2008, S. 60.

[50] Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Aufl. 2010, Artikel 16 Rn. 48.

[51] Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Aufl. 2010, Artikel 16 Rn. 50.

[52] Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Gesamtkonzept für den Datenschutz in der Europäischen Union", KOM (2010) 609, online abrufbar unter: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf

[53] Vgl. Roßnagel, Alexander: Anmerkung zu EuGH Urteil vom 6. November 2003, C-101/01, Slg. 2003, I-12971 Rn 87 – Lindqvist = MMR 2004, 95 (99).

[54] EuGH, Urteil vom 20. Mai 2003, Rs. C-465/00, Slg. I-04989 - Österreichischer Rundfunk.

[55] Dieses weite Verständnis des Anwendungsbereichs der Richtlinie trägt nach Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sehr zur „Europäisierung des Datenschutzes" bei, vgl.: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: Pflicht des österreichischen Rundfunks zur namentlichen Mitteilung der Arbeitnehmerjahresbezüge ab einer bestimmten Grenzen an den Rechnungshof zur Aufnahme in einem öffentlichen Bericht („ORF") (EuGH). http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/Arbeit/Artikel/200503_OesterreichischerRundfunk.html?nn=408918

[56] EuGH, Urteil vom 6. November 2003, C-101/01, Slg. 2003, I-12971 – Lindqvist.

[57] EuGH, Urteil vom 30. Mai 2006, verb. Rs. C-317/04 und C-318/04, Slg. 2006, I-4721 – Europäisches Parlament gegen Rat der EU.

[58] Siehe auch Artikel 3 Absatz 2 zweiter Spiegelstrich DSRL.

[59] EuGH, Urteil vom 10. Februar 2009, Rs. C-301/06, MMR 2009, 244 ff. – Vorratsdatenspeicherung.

Grundrechtliche Fragen waren hingegen nicht Gegenstand des Verfahrens. Die Vorratsdatenspeicherungsrichtlinie stelle keine Regelung der Strafverfolgung dar, sondern habe – anders als bei der Fluggastdatenübermittlung – den Zweck, durch Harmonisierung das Handeln der Telekommunikationsdienstleister im Binnenmarkt zu erleichtern. Die Richtlinie sei daher zu Recht auf der Grundlage der Binnenmarktkompetenz erlassen worden. Anders als mit der Klage geltend gemacht, sei ein Rahmenbeschluss nach den Bestimmungen über die polizeiliche und justizielle Zusammenarbeit nicht erforderlich.

Im Hinblick auf das zentrale deutsche Ausländerregister entschied der EuGH mit Urteil vom 16. Dezember 2008[60], dass die Speicherung und Verarbeitung personenbezogener Daten namentlich genannter Personen zu statistischen Zwecken nicht dem Erforderlichkeitsgebot[61] im Sinne der Datenschutzrichtlinie entspreche und die Nutzung der im Register enthaltenen Daten zur Bekämpfung der Kriminalität gegen das Diskriminierungsverbot verstoße. Denn diese Nutzung stelle auf die Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit ab. Ein System zur Verarbeitung personenbezogener Daten, das der Kriminalitätsbekämpfung diene, aber nur EU-Ausländer erfasse, sei mit dem Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit unvereinbar.

Zum Verhältnis von Pressefreiheit und Datenschutz äußerte sich der EuGH in seiner Entscheidung vom 16. Dezember 2008[62]. Das Unternehmen Markkinapörrsi veröffentlichte Steuerdaten (Namen und Einkommen), die bei den finnischen Steuerbehörden öffentlich zugänglich waren. Der EuGH sah auch diese Weiterveröffentlichung bereits öffentlich zugänglicher Informationen als Datenverarbeitung im Sinne der Datenschutzrichtlinie an. Um Datenschutz und Meinungsfreiheit in Ausgleich zu bringen, seien die Mitgliedstaaten aufgerufen, Einschränkungen des Datenschutzes vorzusehen. Diese seien jedoch nur zu journalistischen, künstlerischen oder literarischen Zwecken, die unter das Grundrecht der Meinungsfreiheit fallen, zulässig. In Anbetracht der hohen Bedeutung der Meinungsfreiheit müsse der Begriff des Journalismus und damit zusammenhängende Begriffe weit ausgelegt werden. Andererseits müssten sich Einschränkungen des Datenschutzes aus Gründen der Meinungsfreiheit auf das absolut Notwendige beschränken.

Mit Urteil vom 9. März 2010 entschied der EuGH in einem Vertragsverletzungsverfahren, das die EU-Kommission gegen Deutschland angestrengt hatte.[63] Die organisatorische Einbindung der Datenschutzaufsicht für den nicht-öffentlichen Bereich in die Innenministerien einiger Bundesländer sowie die Aufsicht der Landesregierungen über die Datenschutzbehörden entspreche nicht den Vorgaben der Datenschutzrichtlinie. Vielmehr sei nach Artikel 28 DSRL erforderlich, dass diese Stellen ihre Aufgabe „in völliger Unabhängigkeit“ wahrnähmen.

Um den Widerstreit von Transparenz und Datenschutz geht es in der Rechtssache Bavarian Lager vom 29. Juni 2010.[64] Die EU-Kommission hatte es abgelehnt, gegenüber der Gesellschaft Bavarian Lager Company die Namen der Teilnehmer eines im Rahmen eines Vertragsverletzungsverfahrens abgehaltenen vertraulichen Treffens offenzulegen. Die Kommission berief sich darauf, dass der Zugang zu Dokumenten nur unter Beachtung des Datenschutzes zulässig sei. Das Europäische Gericht hatte 2007 in erster Instanz entschieden, dass die Herausgabe der Dokumente nur dann verweigert werden könne, wenn der Schutz der Privatsphäre verletzt werde. Das sei bei einer bloßen Namensnennung auf einer Teilnehmerliste im beruflichen Kontext nicht der Fall. Auf der Grundlage der Datenschutzverordnung für die EU-Organe sowie der Verordnung 1049/2001/EG[65] entschied der EuGH im Juni 2010, dass die Kommission rechtmäßig gehandelt habe. Die in dem Sitzungsprotokoll aufgeführten Teilnehmernamen seien personenbezogene Daten. Da Bavarian Lager Argumente für die Notwendigkeit der Übermittlung dieser Daten oder ein berechtigtes Interesse nicht vorgetragen habe, könne die Kommission keine Interessenabwägung vornehmen. Die Verpflichtung zur Transparenz sei daher im konkreten Fall von der Kommission hinreichend gewahrt worden.

Demgegenüber sah das Gericht bei der Internetveröffentlichung der Namen aller natürlichen Personen, die EU-Agrarsubventionen empfangen haben, den Grundsatz der Verhältnismäßigkeit verletzt. Denn hierbei wurde nicht nach einschlägigen Kriterien wie Häufigkeit oder Art und Höhe der Beihilfen unterschieden. Das Interesse der Steuerzahler an Informationen über die Verwendung öffentlicher Gelder rechtfertige einen solchen Eingriff in das Recht auf Schutz der personenbezogenen Daten nach Artikel 8 GRC nicht.[66]

1.3 Nationales Recht

1.3.1 Grundrechte

Das Grundgesetz kennt kein ausdrückliches Datenschutzgrundrecht. Allerdings hat das Bundesverfassungsgericht bereits 1983 in seinem so genannten Volkszählungsurteil[67] das Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG) formuliert. Forderungen, den Datenschutz

---

[60] EuGH, Urteil vom 16. Dezember 2008, Rs. C-524/06, MMR 2009, 171 ff. – Huber.

[61] Artikel 7 Buchstabe e DSRL.

[62] EuGH, Urteil vom 16. Dezember 2008, Rs. C-73/07, Slg. 2007, I-7075 – Markkinapörrsi.

[63] EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland.

[64] EuGH, Urteil vom 29. Juni 2010, Rs. C-28/08, EuZW 2010, 617 – Bavarian Lager Company.

[65] Verordnung des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den öffentlichen Zugang zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission, ABl. EG Nr. L 145, S. 43.

[66] EuGH, Urteil vom 9. November 2010, Rs. C-92/09, C-93/09, EuZW 2010, 939 – Scheck GbR und Eifert gegen Land Hessen.

[67] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1 – Volkszählung.

ausdrücklich als Grundrecht im Grundgesetz zu verankern, fanden bisher nicht die erforderliche Mehrheit.[68] Nach der Rechtsprechung des Bundesverfassungsgerichts beinhaltet das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[69] Die Unsicherheit, wo welche personenbezogenen Informationen gespeichert, verwendet oder weitergegeben werden, würde „nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[70] „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.[71] In den Schutzbereich dieses Grundrechts fallen alle Formen der Erhebung personenbezogener Daten. Angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie geht das Bundesverfassungsgericht davon aus, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr“ gebe.[72]

Im Hinblick auf die Fragestellungen der Enquete-Kommission Internet und digitale Gesellschaft sind als weitere Ausprägungen des allgemeinen Persönlichkeitsrechts das Recht am eigenen Bild von Bedeutung, das unter anderem den Einzelnen vor der Aufnahme, Darbietung, Verbreitung und sonstigen Verwertung seines Abbildes schützt[73], sowie das 2008 durch das Bundesverfassungsgericht formulierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[74] Nach der Rechtsprechung des Gerichts handelt es sich hierbei um ein subsidiäres Grundrecht, das hinter anderen Grundrechten, etwa dem Brief-, Post- und Fernmeldegeheimnis (Artikel 10 GG) oder der Unverletzlichkeit der Wohnung (Artikel 13 GG) zurücktritt und erst dann zur Anwendung kommt, wenn vorrangige Grundrechte keinen hinreichenden Schutz vor Eingriffen in informationstechnische Systeme gewähren.[75]

Grundlegend für den Datenschutz sind weiterhin die Grundrechte nach Artikel 10 GG (Brief-, Post- und Fernmeldegeheimnis, auch als „Telekommunikationsgeheimnis“ bezeichnet) und Artikel 13 GG (Unverletzlichkeit der Wohnung). Das Grundrecht der Unverletzlichkeit der Wohnung schützt unter anderem vor Durchsuchungen und Abhörmaßnahmen, etwa wenn hierfür in die Wohnung eingedrungen wird.[76]

Durch das Fernmeldegeheimnis wird die unbeobachtete, nicht öffentliche Kommunikation unabhängig von der Übertragungsart (Kabel, Funk, analoge oder digitale Vermittlung) und unabhängig von deren Ausdrucksformen (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) geschützt, und zwar auch über das Internet, beispielsweise als E-Mail.[77] Der Schutz erstreckt sich nicht nur auf die Inhalte der Kommunikation, sondern auch auf die Kommunikationsumstände[78], etwa die beteiligten Personen, Zeit, Ort und Häufigkeit der Kommunikation. An Artikel 10 GG zu messen ist weiterhin der Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen von geschützten Kommunikationsvorgängen anschließt, sowie der Gebrauch, der von den so erlangten Kenntnissen gemacht wird.[79] Da das Telekommunikationsgeheimnis vorrangig vor der Manipulation des technischen Übertragungsvorgangs schützt, endet der Schutz des Fernmeldegeheimnisses, sobald der Übertragungsvorgang abgeschlossen ist. Bezogen auf die Telekommunikation enthält Artikel 10 GG eine spezielle Garantie, die das Recht auf informationelle Selbstbestimmung verdrängt und aus der sich besondere Anforderungen für die Daten ergeben, die durch Eingriffe in das Fernmeldegeheimnis erlangt werden. Nach der Rechtsprechung des Bundesverfassungsgerichts lassen sich allerdings die Maßgaben, die für das Recht auf informationelle Selbstbestimmung gelten, grundsätzlich auf Eingriffe in das Fernmeldegeheimnis übertragen, soweit dieser die Erlangung personenbezogener Daten betrifft.[80]

1.3.2 Einfaches Bundesrecht

Das Bundesdatenschutzgesetz (BDSG)[81] stellt das Kernstück des Datenschutzrechts auf Bundesebene dar. Es wurde 1990 als umfassende Novelle des Bundesdatenschutzgesetzes von 1977 in Reaktion auf das Volkszählungsurteil verabschiedet, um – den Vorgaben des Bundesverfassungsgerichts entsprechend – eine gesetzliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten zu schaffen und so den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechtes zu

---

[68] Viele Landesverfassungen enthalten hingegen ein eigenständiges Datenschutzgrundrecht, vgl. die Landesverfassungen von Berlin (Artikel 33), Brandenburg (Artikel 11), Bremen (Artikel 12), Mecklenburg-Vorpommern (Artikel 6), Nordrhein-Westfalen (Artikel 4), Rheinland-Pfalz (Artikel 4a), Saarland (Artikel 2), Sachsen (Artikel 33), Sachsen-Anhalt (Artikel 6) und Thüringen (Artikel 6). Vgl. im Übrigen Kapitel 2.2.2.

[69] BVerfGE 65, 1, 45 – Volkszählung.

[70] BVerfGE 65, 1, 43 – Volkszählung.

[71] BVerfGE 65, 1, 43 – Volkszählung.

[72] BVerfGE 65, 1, 45 – Volkszählung. Zum Grundrecht auf informationelle Selbstbestimmung vgl. im Übrigen Kapitel 2.1.5.

[73] Vgl. Di Fabio, Udo, in: Maunz, Theodor/Dürig, Günter. Grundgesetz. 57. Auflage 2010, Artikel 2 Rn. 193.

[74] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370, 595/07, BVerfGE 120, 274, 302 ff. – Onlinedurchsuchung.

[75] Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vgl. im Übrigen Kapitel 2.1.3.

[76] BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, BVerfGE 109, 279 – Großer Lauschangriff.

[77] BVerfGE 120, 274, 307 – Onlinedurchsuchung.

[78] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04, BVerfGE 113, 348, 364 – Vorbeugende Telekommunikationsüberwachung.

[79] BVerfGE 113, 348, 365 – Vorbeugende Telekommunikationsüberwachung.

[80] BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, NJW 2007, 351 (354 f).

[81] Gesetz vom 20. Dezember 1990 in der Fassung der Bekanntmachung vom 14. Januar 2003, BGBl. I, S. 66, zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009, BGBl. I, S. 2814.

schützen. Als Teil des allgemeinen Datenschutzrechts enthält es keine bereichsspezifischen Regelungen und gilt sowohl für Datenverarbeitung in IT-Systemen als auch auf für manuelle Verfahren.

Geschützt werden vom Gesetz „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Absatz 1 BDSG), nicht aber Angaben über juristische Personen. Wesentlicher Grundsatz des Gesetzes ist das so genannte Verbot mit Erlaubnisvorbehalt nach § 4 Absatz 1 BDSG. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn ein Gesetz oder eine sonstige Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Daneben gilt der Grundsatz der Datenvermeidung und Datensparsamkeit, wonach so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen sind. Möglichkeiten der Anonymisierung und Pseudonymisierung sind weitestgehend auszuschöpfen. Das Gesetz stellt für „besondere Arten personenbezogener Daten“, etwa über die rassische oder ethnische Herkunft, politische Meinungen oder religiöse Überzeugungen, höhere Schutzanforderungen. Rechte des Betroffenen erstrecken sich auf Auskunft, Berichtigung, Löschung oder Sperrung. Der zentrale datenschutzrechtliche Grundsatz der Zweckbindung hat an verschiedenen Stellen im Gesetz Niederschlag gefunden. Das Datenschutzaudit ist Gegenstand der Regelung des § 9a BDSG.

Neben allgemeinen und gemeinsamen Bestimmungen enthält das Gesetz gesonderte Regelungen für die Datenverarbeitung öffentlicher Stellen einerseits und nicht-öffentlicher Stellen andererseits. Die Regelungen über die Datenverarbeitung öffentlicher Stellen (§§ 12 ff. BDSG) gelten für Behörden und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, bundesunmittelbare öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen sowie Organe der Rechtspflege. Für öffentliche Stellen der Länder gelten sie stets nur subsidiär gegenüber den Landesdatenschutzgesetzen. Da alle Bundesländer Landesdatenschutzgesetze erlassen haben, ergibt sich hierfür kein praktischer Anwendungsfall. Wahl, Rechtsstellung und Aufgabe des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind in §§ 22 ff. BDSG geregelt. Das Gesetz enthält weiterhin Bußgeld- und Strafvorschriften.

Der räumliche Anwendungsbereich des BDSG ist in § 1 Absatz 5 BDSG geregelt. Erhebt oder verarbeitet ein ausländisches Unternehmen mit Sitz innerhalb der EU beziehungsweise innerhalb des Europäischen Wirtschaftsraums (EWR) Daten im Inland, ist das Bundesdatenschutzgesetz nur dann anwendbar, wenn das Unternehmen durch eine deutsche Niederlassung tätig wird. Bei Datenerhebung und -verarbeitung im Inland durch ein Unternehmen mit Sitz außerhalb der EU beziehungsweise außerhalb des EWR findet das Bundesdatenschutzgesetz hingegen Anwendung.[82]

[82] Anderes gilt nach § 1 Absatz 5 S. 4 BDSG im Fall des „Transits“.

Gegenüber spezielleren Vorschriften des Bundesrechts tritt das Bundesdatenschutzgesetz zurück (§ 1 Absatz 3 BDSG). Wegen zahlreicher bereichsspezifischer Regelungen in anderen Gesetzen wird das BDSG daher als Auffanggesetz des insgesamt zersplitterten Datenschutzrechts angesehen.[83] Beispiele für Spezialregelungen sind das Bundespolizeigesetz, das Bundeskriminalamtsgesetz, das Bundeszentralregistergesetz, das Personenstandsgesetz, §§ 8 ff. Handelsgesetzbuch und die Grundbuchordnung.[84] In gesonderten Vorschriften außerhalb des Bundesdatenschutzgesetzes ist auch der Datenschutz der öffentlich-rechtlichen Religionsgemeinschaften geregelt. Im Zehnten Buch des Sozialgesetzbuchs (SGB X, Zweites Kapitel „Schutz der Sozialdaten“, §§ 67 ff.)[85] finden sich die datenschutzrechtlichen Bestimmungen für den Sozialleistungsbereich. Sozialdaten sollen nach der Vorstellung des Gesetzgebers einem erhöhten, dem Steuergeheimnis vergleichbaren Schutz unterliegen.[86] Ergänzende Bestimmungen für verschiedene Zweige der Sozialversicherung enthalten die jeweils einschlägigen Bücher des Sozialgesetzbuchs.

Für das Internet von besonderer Bedeutung ist das Telemediengesetz (TMG).[87] Telemedien sind Waren- und Dienstleistungsangebote im Netz unter Einbeziehung redaktionell gestalteter Online-Angebote, ausgenommen jedoch der Rundfunk.[88] Für diese Medien enthält das Telemediengesetz Vorschriften über den Umgang mit personenbezogenen Nutzerdaten (§§ 11 ff. TMG). Auch im Telemediengesetz gelten die Grundsätze der Zweckbindung, der Datenvermeidung und -sparsamkeit. Den allgemeinen Datenschutzgrundsätzen folgend, ist im Bereich der Telemedien die Erhebung und Verarbeitung personenbezogener Daten nur mit Einwilligung der Betroffenen oder auf gesetzlicher Grundlage zulässig. Zugeschnitten auf den Bereich der Telemedien sind in § 13 TMG die Voraussetzungen für eine elektronische Einwilligung geregelt. Über Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen Diensteanbieter und Nutzern erforderlich sind (Bestandsdaten), darf der Dienstanbieter nach § 14 TMG auf Anordnung der zuständigen Stellen im Einzelfall Auskunft erteilen, etwa zum Zwecke der Strafverfolgung, zur Gefahrenabwehr, zur Terrorbekämpfung oder zur Durchsetzung der Rechte am geistigen Eigentum.

Telekommunikationsdienste sind hingegen solche Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsdienste bestehen,

[83] Vgl. Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 1 Rn. 14.

[84] Vgl. Däubler, Wolfgang/u.a. (Hrsg.). Bundesdatenschutzgesetz – Kommentar. 3. Auflage 2010, Einleitung, Rn. 73.

[85] Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I, S. 130), zuletzt geändert durch Gesetz vom 5. August 2010, BGBl. I, S. 1127.

[86] Bundestagsdrucksache 8/4022, S. 96.

[87] Telemediengesetz vom 26. Februar 2007, BGBl. I, S. 179, zuletzt geändert durch Gesetz vom 14. August 2009, BGBl. I, S. 2814.

[88] Vgl. Hoeren, Thomas: Das Telemediengesetz. NJW 2007, 801 (801).

darunter nach Vorstellung des Gesetzgebers auch Internet-Telefonie, Internetzugang und E-Mail-Übertragung.[89] Der Datenschutz für die Teilnehmer ist im Telekommunikationsgesetz (TKG)[90], insbesondere §§ 91 ff. TKG, geregelt. Geschützt sind Angaben über persönliche und sachliche Verhältnisse, unter anderem Informationen über das Kommunikationsverhalten, das heißt „wer wann mit wem von welchem Anschluss aus telefoniert hat."[91] Das Telekommunikationsgesetz enthält Regelungen unter anderem über Bestands- und Verkehrsdaten, Entgeltermittlung und -abrechnung.

1.3.3 Landesrecht

Die Landesdatenschutzgesetze gelten für die Verarbeitung personenbezogener Daten durch die jeweiligen Landesbehörden und andere öffentlich-rechtliche Einrichtungen der Länder. Sie enthalten Bestimmungen über die Landesdatenschutzbeauftragten. Ganz überwiegend gilt auch für die Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen Regelungen.[92] Da der Datenschutz in nahezu allen Bereichen der Landesverwaltung von Bedeutung ist, weist eine Unzahl landesrechtlicher Gesetze Spezialregelungen zum Datenschutz auf, unter anderem die Landesgesetze zum (Jugend-)Strafvollzug und zur Untersuchungshaft, die Rettungsdienstgesetze, Brand- und Katastrophenschutzgesetze sowie die Schulgesetze.

Anders als im Bundesrecht finden sich auf Landesebene auch Formen untergesetzlicher Regelungen zum allgemeinen Datenschutzrecht, das heißt Rechtsverordnungen und Verwaltungsvorschriften.[93]

1.3.4 Rechtsprechung des Bundesverfassungsgerichts

Neben den unter 1.3.1 erwähnten grundlegenden Entscheidungen, dem Volkszählungsurteil sowie dem Urteil zur „Onlinedurchsuchung", hat sich das Bundesverfassungsgericht in einer Reihe weiterer Entscheidungen mit Fragen der informationellen Selbstbestimmung und verwandter Grundrechte befasst. Seine Rechtsprechung enthält im Bereich des Datenschutzes vielfach sehr konkrete und detaillierte Vorgaben für das gesetzgeberische Handeln.[94] Aus der umfangreichen Rechtsprechung des Gerichts zum Datenschutz sei beispielhaft auf folgende Entscheidungen hingewiesen:

Gegenstand eines Urteils vom 14. Juli 1999[95] waren erweiterte Befugnisse des Bundesnachrichtendienstes zur Überwachung, Aufzeichnung und Auswertung des Telekommunikationsverkehrs sowie zur Übermittlung der daraus erlangten Daten an andere Behörden. 1994 war das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) mit dem Ziel geändert worden, Informationen unter anderem im Bereich des internationalen Terrorismus, des Drogenhandels und der Geldwäsche zu erlangen, um sie nachfolgend den zuständigen Behörden zur Verhinderung, Aufklärung und Verfolgung von Straftaten zur Verfügung zu stellen.[96] Mit Beschluss vom 5. Juli 1995[97] bestimmte das Bundesverfassungsgericht im Rahmen einer einstweiligen Anordnung, dass einzelne der neugefassten Vorschriften zunächst nur eingeschränkt angewendet werden dürften. In der Hauptsache urteilte das Gericht im Jahr 1999, dass einzelne Vorschriften gegen Artikel 10 GG verstießen. Das Fernmeldegeheimnis schütze in erster Linie den Kommunikationsinhalt vor staatlicher Kenntnisnahme, daneben aber auch die Kommunikationsumstände. Der Schutz erstrecke sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen von geschützten Kommunikationsvorgängen anschließe, und den Gebrauch, der von den erlangten Kenntnissen gemacht werde. Solle der Bundesnachrichtendienst zu Eingriffen in das Fernmeldegeheimnis ermächtigt werden, sei der Gesetzgeber verpflichtet, Vorsorge gegen Gefahren zu treffen, die sich aus der Erhebung und Verwertung personenbezogener Daten ergeben. Hierzu verwies das Gericht auf die im Volkszählungsurteil entwickelten Kriterien für Eingriffe in Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG. Diese seien auch auf die speziellere Regelung des Artikel 10 GG übertragbar. Speicherung und Verwendung erlangter Daten seien grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt habe. Zweckänderungen seien nur durch Allgemeinbelange gerechtfertigt, die die grundrechtlich geschützten Interessen überwiegen. Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken sei mit diesen Vorgaben unvereinbar.

Mit Beschluss vom 14. Dezember 2000[98] konstatierte das Gericht, dass die Feststellung, Speicherung und künftige Verwendung des „genetischen Fingerabdrucks" auf der Grundlage von § 81g Strafprozessordnung (StPO) und § 2 DNA-Identitätsfeststellungsgesetz[99] in das Recht auf informationelle Selbstbestimmung eingreife, es sich aber um einen rechtlich zulässigen Grundrechtseingriff handele, da unter anderem das Gebot der Normenklarheit,

---

89 Bundestagsdrucksache 16/3078, S. 13.
90 Telekommunikationsgesetz vom 25. Juni 1996, BGBl. I, S. 1120, geändert durch Gesetz vom 22. Juni 2004, BGBl. I, S. 1190. Zur geplanten TKG-Novelle vgl. auch Fn. 42.
91 Robert, Anna, in: Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.). Beck'scher TKG-Kommentar. 3. Auflage 2006, § 91 Rn. 12.
92 Vgl. Gola, Peter/Schomerus, Rudolf: BDSG. Kommentar. 10. Auflage 2010, § 1 Rn. 33.
93 Vgl. Däubler, Wolfgang/u.a. (Hrsg.). Bundesdatenschutzgesetz – Kommentar. 3. Auflage 2010, Einleitung, Rn. 70.
94 Vgl. Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035; Wolff, Heinrich A.: Vorratsdatenspeicherung. NVwZ 2010, 751.
95 BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, BVerfGE 100, 313 ff. – Telekommunikationsüberwachung.
96 Verbrechensbekämpfungsgesetz vom 28. Oktober 1994, BGBl. I, S. 3186.
97 BVerfG, Beschluss vom 5. Juli 1995 – 1 BvR 2226/94, BVerfGE 93, 181 – Rasterfahndung I.
98 BVerfG, Beschluss vom 14. Dezember 2000 – 2 BvR 1741/99, 276, 2061/00, BVerfGE 103, 21 – Genetischer Fingerabdruck I.
99 Aufgehoben mit Wirkung vom 1. November 2005.

das Übermaßverbot und der Richtervorbehalt gewahrt seien.

In einem Urteil vom 12. April 2005[100] äußerte sich das Bundesverfassungsgericht zu einer weiteren Vorschrift der Strafprozessordnung. Gesetzliche Grundlage für Beweiserhebungen unter Einsatz eines satellitengestützten Ortungssystems (Global-Positioning-System, GPS) und die Verwertung der Erkenntnisse war im zugrunde liegenden Sachverhalt § 100c Absatz 1 Nummer 1 Buchstabe b StPO damaliger Fassung, wonach ohne Wissen des Betroffenen „besondere für Observationszwecke bestimmte technische Mittel“ eingesetzt werden konnten. Die Vorschrift sei verfassungsgemäß, da sie hinreichend bestimmt sei und nicht in den unantastbaren Kernbereich privater Lebensgestaltung eingreife. Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels sei der Gesetzgeber aber aufgerufen, die technischen Entwicklungen aufmerksam zu verfolgen und notfalls korrigierend einzugreifen.

Die Durchsuchung und Beschlagnahme des gesamten elektronischen Datenbestands einer gemeinsam betriebenen Rechtsanwaltskanzlei und Steuerberatungsgesellschaft – im Rahmen eines gegen einen der Berufsträger gerichteten Ermittlungsverfahrens – qualifizierte das Bundesverfassungsgericht mit Beschluss vom 12. April 2005[101] als erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung. Dem müsse durch strikte Beachtung des Verhältnismäßigkeitsgrundsatzes und bestimmter Verfahrensregelungen Rechnung getragen werden. Zu berücksichtigen sei unter anderem, dass das Vertrauensverhältnis zwischen Rechtsanwälten und Mandanten rechtlich besonders geschützt und durch die Streubreite der sichergestellten Daten eine Vielzahl gänzlich unbeteiligter Personen von der Beschlagnahme betroffen sei.

Zu den verfassungsrechtlichen Grenzen der Rasterfahndung, bei der den Polizeibehörden von anderen Stellen personenbezogene Daten übermittelt und nachfolgend einem automatisierten Abgleich nach bestimmten Merkmalen unterzogen werden, hat das Bundesverfassungsgericht mit Beschluss vom 4. April 2006 entschieden. Eine präventive polizeiliche Rasterfahndung stelle einen Grundrechtseingriff von besonderer Intensität dar und sei daher mit dem Grundrecht auf informationelle Selbstbestimmung nur dann vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben sei.[102] Eine allgemeine Bedrohungslage, wie etwa seit dem 11. September 2001, ohne das Vorliegen weiterer Tatsachen, sei dafür nicht ausreichend.

Mit Beschluss vom 13. Juni 2007[103] erklärte das Gericht Vorschriften zum automatischen Kontenabruf teilweise für verfassungswidrig, da gegen den verfassungsrechtlichen Bestimmtheitsgrundsatz verstoßen werde. Die angegriffenen Regelungen ermächtigten einzelne Behörden zur automatisierten Abfrage von Daten, die von den Kreditinstituten vorgehalten werden müssen. Soweit das Gebot der Normenklarheit nicht eingehalten worden sei, verstoße die Regelung gegen das Recht auf informationelle Selbstbestimmung. Einen solchen Verstoß bejahte das Gericht hinsichtlich § 93 Absatz 8 Abgabenordnung (AO) damaliger Fassung, da der Kreis der zur Kontenabfrage berechtigten Behörden und die dabei verfolgten Zwecke nicht hinreichend festgelegt worden seien.

Auch eine Geschwindigkeitsmessung auf der Grundlage einer Verwaltungsvorschrift stellt nach der Rechtsprechung des Bundesverfassungsgerichts eine unzulässige Einschränkung des Rechts auf informationelle Selbstbestimmung dar[104], da eine solche Maßnahme nur auf gesetzlicher Grundlage, die dem Gebot der Normenklarheit und Verhältnismäßigkeit zu entsprechen habe, zulässig sei.

Die Einführung der Vorratsdatenspeicherung durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung“[105] zur Umsetzung der Vorratsdatenspeicherungsrichtlinie in deutsches Recht ist Gegenstand mehrerer Entscheidungen des Bundesverfassungsgerichts. Nach § 113a TKG waren Telekommunikationsdiensteanbieter verpflichtet, Verkehrsdaten von Telefondiensten (Festnetz, Mobilfunk, Fax, SMS, MMS), E-Mail-Diensten und Internetdiensten vorsorglich anlasslos für die Dauer von sechs Monaten zu speichern. Die zulässigen Zwecke der Datenverwendung waren in § 113b TKG, die Verwendung der Daten für die Strafverfolgung in § 100g StPO geregelt. Nachdem das Gericht mit Beschluss vom 28. Oktober 2008[106] im Wege der einstweiligen Anordnung Teile der Vorratsdatenspeicherung außer Kraft gesetzt hatte, entschied es mit Urteil vom 2. März 2010[107] in der Hauptsache, dass die Regelungen des Telekommunikationsgesetzes und der Strafprozessordnung über die Vorratsdatenspeicherung mit Artikel 10 Absatz 1 GG unvereinbar und damit nichtig seien. Die Vorratsdatenspeicherung durch private Telekommunikationsunternehmen greife in den Schutzbereich des Fernmeldegeheimnisses ein, da diese als „Hilfspersonen“ für die Aufgabenerfüllung staatlicher Behörden in Anspruch genommen würden. Zwar sei eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehle aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Datensicherheit, Begrenzung der Verwendungszwecke, verfassungsrechtliche Transparenz und Rechtschutzanforderungen seien nicht hinreichend gewährleistet.

---

[100] BVerfG, Urteil vom 12. April 2005 – 2 BvR 581/01, BVerfGE 112, 304 – GPS-Überwachung.

[101] BVerfG, Beschluss vom 12. April 2005 – 2 BvR 1027/02, BVerfGE 113, 29, 46 – Beschlagnahme von Datenträgern.

[102] BVerfGE 93, 181 – Rasterfahndung I.

[103] BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03, NJW 2007, 2464 – Automatisierte Abfrage von Kontostammdaten.

[104] BVerfG, Beschluss vom 11. August 2009 – 2 BvR 941/08, NJW 2009, 3293 – Verkehrsüberwachung.

[105] Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007, BGBl. I, S. 3198.

[106] BVerfG, Beschluss vom 28. Oktober 2008 – 1 BvR 256/08, BVerfGE 122, 120 – Vorratsdatenspeicherung/Datenermittlung.

[107] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 – Vorratsdatenspeicherung.

Für die Frage, zum Schutz welcher Rechtsgüter der Datenabruf als verhältnismäßig anzusehen ist, differenziert das Gericht zwischen der unmittelbaren und mittelbaren Nutzung der Daten. Der Abruf und die unmittelbare Nutzung der Daten seien nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienten. Im Bereich der Strafverfolgung setze dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürften diese Maßnahmen nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden.

Soweit die Behörden in §§ 113b Satz 1, Halbsatz 2, 113 TKG zur Identifizierung von IP-Adressen berechtigt wurden, von Diensteanbietern auf der Grundlage gespeicherter Verkehrsdaten die Identität bestimmter, bereits bekannter IP-Adressen zu erfragen, sei diese nur mittelbare Nutzung der Daten auch unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung, Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die Verfolgung von Ordnungswidrigkeiten könnten solche Auskünfte hingegen nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden.

1.3.5 Rechtsprechung nationaler Verwaltungs- und Zivilgerichte

Zulässigkeit und Grenzen personenbezogener Bewertungsportale im Internet sind Gegenstand einer Entscheidung des Bundesgerichtshofs (BGH) vom 23. Juni 2009[108]. Der Bundesgerichtshof lehnte einen Anspruch der klagenden Lehrerin auf Löschung oder Unterlassung der Veröffentlichung ihres Namens, des Namens der Schule, der unterrichteten Fächer sowie einer Bewertung durch die Nutzer ab. Auch Meinungsäußerungen über eine bestimmte oder bestimmbare Person oder diesbezügliche Bewertungen stellten personenbezogene Daten dar. Die Erhebung, Speicherung und Übermittlung solcher Beurteilungen richte sich daher nach dem Bundesdatenschutzgesetz. Im konkreten Fall sei die Erhebung und Speicherung der Bewertung trotz fehlender Einwilligung der Lehrerin gemäß § 29 BDSG zulässig. Voraussetzung hierfür ist nach § 29 BDSG, dass „kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss“ der Datenerhebung und -speicherung hat. Bei der Prüfung des „schutzwürdigen Interesses“ hat der Bundesgerichtshof eine Abwägung zwischen der Meinungsfreiheit der Nutzer aus Artikel 5 Absatz 1 GG und dem Persönlichkeitsrecht der Bewerteten vorgenommen und im Hinblick auf den konkreten Sachverhalt der Meinungsfreiheit den Vorrang eingeräumt.[109]

Mit Urteil vom 9. Dezember 2003[110] lehnte der Bundesgerichtshof zivilrechtliche Ansprüche auf Unterlassung ab, mit denen die Presseveröffentlichung von Luftbildaufnahmen, die Privathäuser einer Prominenten zeigten, verhindert werden sollte. Das Fotografieren der Außenansicht eines Grundstücks von einer allgemein zugänglichen Straße aus und die Verbreitung dieser Fotos stelle regelmäßig keine Verletzung des Persönlichkeitsrechts dar. Wenn aber jemand „unter Überwindung bestehender Hindernisse oder mit geeigneten Hilfsmitteln (Teleobjektiv, Leiter, Flugzeug)“ ein privates Anwesen ausspähe, liege grundsätzlich ein Eingriff in die Privatsphäre vor. Im konkreten Fall hat das Gericht dennoch einen Unterlassungsanspruch verneint, da bei Abwägung der betroffenen Grundrechte die Pressefreiheit aus Artikel 5 Absatz 1 GG überwiege. Von der Pressefreiheit nicht gedeckt sei aber die Veröffentlichung einer Wegbeschreibung zum Grundstück. Auch die Installation von Überwachungskameras auf einem Privatgrundstück kann das Persönlichkeitsrecht eines vermeintlich überwachten Nachbars beeinträchtigen.[111]

Zur Frage der internationalen Zuständigkeit deutscher Gerichte gemäß § 32 Zivilprozessordnung (ZPO) für Klagen aus unerlaubten Handlungen gegen Veröffentlichungen im Internet hat sich der Bundesgerichtshof mit Urteil vom 29. März 2011[112] geäußert. Deutsche Gerichte seien für Verletzungen des Persönlichkeitsrechts durch Veröffentlichungen im Internet dann zuständig, wenn die fraglichen Inhalte „objektiv einen deutlichen Bezug zum Inland […] aufweisen“. Voraussetzung hierfür sei, dass eine Kollision der widerstreitenden Interessen, das heißt des Persönlichkeitsrechts einerseits und des Interesses an der Gestaltung des eigenen Internetauftritts oder an der Berichterstattung andererseits, nach den Umständen des konkreten Falls, insbesondere aufgrund des konkreten Inhalts der Veröffentlichung, im Inland tatsächlich eingetreten sei oder eintreten könne. Das hat das Gericht im konkreten Fall verneint, da es sich um die Beschreibung eines privaten Treffens in Russland – verfasst auf russisch und in kyrillischer Schrift – handelte. Aus dem deutschen Wohnsitz des Klägers und dem Standort des Servers in Deutschland ergebe sich kein hinreichend deutlicher Inlandsbezug.

Mit Urteil vom 2. März 2010[113] hat der Bundesgerichtshof die Zuständigkeit deutscher Gerichte für eine Klage gegen eine Internetveröffentlichung der New York Times hingegen bejaht. Der deutliche Inlandsbezug ergab sich nach Auffassung des Gerichts aus dem Inhalt des veröffentlichten Artikels (unter anderem die Wiedergabe von Berichten deutscher Strafverfolgungsbehörden über das deutsche Unternehmen des Klägers) und der Tatsache, dass die New York Times als international anerkannte Zeitung auch in Deutschland wahrgenommen werde.

---

[108] BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich.de.

[109] Die gegen das Urteil eingelegte Verfassungsbeschwerde hat das BVerfG mit Beschluss vom 16. August 2010 nicht zur Entscheidung angenommen (Az. 1 BvR 1750/09).

[110] BGH, Urteil vom 9. Dezember 2003 – VI ZR 404/02, NJW 2004, 766 – Luftbildaufnahmen.

[111] BGH, Urteil vom 16. März 2010 – VI ZR 176/09, NJW 2010, S. 1533 – Überwachungskamera.

[112] BGH, Urteil vom 29. März 2011 – VI ZR 111/10.

[113] BGH, Urteil vom 2. März 2010 – VI ZR 23/09.

In der Rechtsprechung des Bundesarbeitsgerichts (BAG) sind Fragen des Datenschutzes und der Persönlichkeitsrechte unter anderem in folgenden Entscheidungen aufgegriffen worden: Arbeitgeber und Betriebsrat seien grundsätzlich befugt, eine Videoüberwachung im Betrieb einzuführen. Die Zulässigkeit des damit verbundenen Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer richte sich nach dem Grundsatz der Verhältnismäßigkeit.[114] Bei Abschluss von Betriebsvereinbarungen sei gemäß § 75 Absatz 2 Satz 1 Betriebsverfassungsgesetz (BetrVG) die freie Entfaltung der Persönlichkeit der beschäftigten Arbeitnehmer zu schützen und hierbei auch der Grundsatz der Verhältnismäßigkeit zu wahren. Mit Beschluss vom 12. August 2008[115] äußerte sich das Gericht zum Leserecht einzelner Mitglieder des Betriebsrates. Das Recht, die elektronisch gespeicherten Unterlagen des Betriebsrats einzusehen, umfasse auch das Leserecht auf elektronischem Weg, und zwar jederzeit, wie dies in § 34 Absatz 3 BetrVG vorgesehen sei. Dem stünden auch die Schweigepflicht der Mitglieder des Betriebsrats und datenschutzrechtliche Vorschriften nicht entgegen.

Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 8. März 2002[116] die Herausgabe von Stasi-Unterlagen mit personenbezogenen Informationen über Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger in Ausübung ihres Amtes nach der damaligen Fassung des Stasi-Unterlagen-Gesetzes (StUG) für unzulässig erklärt, wenn diese systematisch vom Staatssicherheitsdienst ausgespäht wurden. Im Hinblick auf eine mögliche Änderung des Gesetzes weist das Gericht darauf hin, dass bei der Weitergabe rechtsstaatswidrig erworbener Informationen dem Persönlichkeitsrecht ein höherer Schutz zukomme, als dies bei der sonstigen Veröffentlichung von Informationen über Personen der Zeitgeschichte und Amtsträger in Ausübung ihres Amtes der Fall sei.[117]

Werden personenbezogene Informationen durch eine sachlich unzuständige Behörde weitergegeben, stellt dies einen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung dar. Das Bundesverwaltungsgericht hat hierzu mit Urteil vom 9. März 2005 entschieden, ein Eingriff in das informationelle Selbstbestimmungsrecht sei grundsätzlich auch dann nicht gerechtfertigt, wenn die Daten zwar von einer anderen Behörde rechtmäßig hätten weitergegeben werden dürfen, im konkreten Fall aber eine sachlich unzuständige Behörde gehandelt habe.[118]

Nach § 7 Bundesnachrichtendienstgesetz (BNDG) in Verbindung mit § 15 Absatz 1 Bundesverfassungsschutzgesetz (BVerfSchG) erteilt der Bundesnachrichtendienst den Betroffenen auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten, soweit sie ein besonderes Interesse an der Auskunft darlegen. Das Bundesverwaltungsgericht hat mit Urteil vom 24. März 2010[119] ausgeführt, dass eine Auskunftserteilung unter Berufung auf die in § 15 Absatz 2 BVerfSchG aufgeführten Geheimhaltungsgründe nur dann abgelehnt werden könne, wenn eine Abwägung im Einzelfall ergebe, dass das Auskunftsinteresse zurückstehen müsse. Dagegen erstrecke sich die Auskunftsverpflichtung von vornherein nicht auf die Herkunft der Daten (§ 15 Absatz 3 BVerfSchG).

1.3.6 Verwaltungs- und Anwendungspraxis

Da der Datenschutz in fast allen Bereichen der öffentlichen Verwaltung von Bedeutung ist und hierzu eine Fülle allgemeiner und bereichsspezifischer Regelungen sowohl auf Bundes- wie auf Landesebene existiert, lassen sich allgemeine Feststellungen zur Verwaltungs- und Anwendungspraxis nur schwer treffen, zumal der Schwerpunkt der Datenschutzaufsicht bei den Aufsichtsbehörden der Länder liegt. Insbesondere die staatliche Datenschutzkontrolle der Privatwirtschaft ist Ländersache (§ 38 Absatz 6 BDSG).

Unterschiede in der Verwaltungspraxis, etwa im Bereich von Ermessensentscheidungen, sind daher möglich; das kann insbesondere für deutschlandweit agierende Unternehmen von Bedeutung sein, da diese im Einzelfall der Aufsicht mehrerer Datenschutzbehörden unterliegen. Zwar wird nach langjähriger Praxis die Behörde tätig, in deren Zuständigkeit der Sitz des Unternehmens liegt. Bei Unternehmen mit mehreren selbstständigen Regionalgesellschaften bleibt es dennoch bei der Zuständigkeit mehrerer Aufsichtsbehörden.[120]

---

[114] BAG, Beschluss vom 26. August 2008 – 1 ABR 16/07, BAGE 127, 276 – Videoüberwachung im Betrieb. Die Regelung des § 32 BDSG „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ ist erst nach der Entscheidung am 1. September 2009 in Kraft getreten. Die Vorschrift regelt u. a.: „Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.“

[115] BAG, Beschluss vom 12. August 2009 – 7 ABR 15/08, NZA 2009, 1218.

[116] BVerwG, Urteil vom 8. März 2002 – 3 C 46/01, BVerwGE 116, 104 – Herausgabe von Stasi-Unterlagen.

[117] Der Gesetzgeber hat dem Rechnung getragen und § 32 Absatz 1 StUG dahingehend geändert, dass Unterlagen mit personenbezogenen Informationen ohne Einwilligung der Betroffenen nur zur Verfügung gestellt werden dürfen, „soweit durch deren Verwendung keine überwiegenden schutzwürdigen Interessen der dort genannten Personen beeinträchtigt werden. Bei der Abwägung ist insbesondere zu berücksichtigen, ob die Informationserhebung erkennbar auf einer Menschenrechtsverletzung beruht.“, vgl. Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik in der Fassung der Bekanntmachung vom 18. Februar 1991, BGBl. I, S. 162, geändert durch Artikel 15 Absatz 64 des Gesetzes vom 5. Februar 2009, BGBl. I, S. 160.

[118] BVerwG, Urteil vom 9. März 2005 – 6 C 3/04, NJW 2005, 2330 – Scientology.

[119] BVerwG, Urteil vom 24. März 2010 – 6 A 2/09, DVBl. 2010, 1307 – Auskunftsanspruch BND.

[120] So wurden 2008 von Datenschutzbehörden aus zwölf Bundesländern Bußgelder gegen 35 Vertriebsgesellschaften des Lebensmitteldiscounters Lidl verhängt, vgl. hierzu: WELTONLINE: Spitzelaffäre kostet Lidl 1,5 Millionen Euro. Artikel vom 11. September 2008. http://www.welt.de/wirtschaft/article2428529/Spitzelaffaere-kostet-Lidl-1-5-Millionen-Euro.html

Die obersten Landesdatenschutzbehörden für die Aufsicht im nicht-öffentlichen Bereich haben deshalb als Koordinierungsgremium den Düsseldorfer Kreis gegründet, dessen Treffen und Beschlüsse eine einheitliche Verwaltungspraxis befördern können. Beschlüsse des Düsseldorfer Kreises, die allerdings Einstimmigkeit voraussetzen, betreffen unterschiedliche Bereiche der Aufsicht, im Jahr 2010 etwa Prüfpflichten von Datenexporteuren im Rahmen des Safe-Harbor-Abkommens.[121]

Bei einer unterschiedlichen Praxis verbleibt es, wenn eine Einigung im Düsseldorfer Kreis nicht zustande kommt. So wird etwa die Praxis von Auskunfteien, vor der Erteilung von Auskünften zur Identitätsüberprüfung die Zusendung einer Kopie des Personalausweises zu verlangen, von den Aufsichtsbehörden teilweise als unzulässig, teilweise aber auch als erforderlich angesehen. Auch bei der Videoüberwachung auf Bahnhöfen gab es unterschiedliche Bewertungen.

2 Datenschutz

2.1 Prinzipien, Ziele, Werte

2.1.1 Schutzgegenstand

Datenschutz bildet den zentralen Motor des Vertrauens und der Akzeptanz moderner informationstechnischer Entwicklungen. Ziel des Datenschutzrechts ist der Erhalt und die Stärkung des Persönlichkeitsrechts unter den Bedingungen der Datenverarbeitung und -erhebung, insbesondere in Gestalt des Rechts auf informationelle Selbstbestimmung. Der Erhalt der Kontrolle über den Umgang mit Daten und Informationen, die einen selbst betreffen, ist das zwingende Äquivalent einer auf die Stärkung des Einzelnen wie auch unseres demokratischen Gemeinwesens insgesamt abzielenden gesellschaftlichen Gesamtentwicklung.

Zentraler Anknüpfungspunkt des bestehenden Datenschutzkonzepts sind die so genannten personenbezogenen Daten.[122] Im Mittelpunkt der Abwägungen des Datenschutzes aber stehen Informationen, nicht Daten. Es geht regelmäßig um Interessen der Grundrechtsträger, dass staatliche Stellen oder Dritte etwas nicht als Information erfahren und nutzen können, und auf der anderen Seite um deren Wissens- und Verwertungsinteressen.

Personenbezogene Daten werden definiert als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (Artikel 2 Buchstabe a DSRL, § 3 Absatz 1 BDSG). Der Begriff wird weit verstanden und umfasst praktisch jede Information, die mit einer natürlichen Person in Verbindung gebracht werden kann. Es genügt also eine „Personenbeziehbarkeit“.[123] Angaben über persönliche Verhältnisse betreffen etwa Identifikationsmerkmale, äußere Merkmale, aber auch innere Zustände (zum Beispiel Meinungen). Unter Angaben über sachliche Verhältnisse werden dagegen alle Beziehungen des Betroffenen zu Dritten und zur Umwelt (zum Beispiel Eigentumsverhältnisse, Vertragsbeziehungen) verstanden.[124]

Auch das Bundesverfassungsgericht geht in seiner ständigen Rechtsprechung von einem weiten Verständnis aus. So hat das Gericht in seinem wegweisenden Volkszählungsurteil zu den Angaben personenbezogener Daten ausgeführt: „Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr.“[125]

Weiterer regulatorischer Anknüpfungspunkt ist der Umgang mit diesen Daten. Dabei werden in der Datenschutzrichtlinie und im Bundesdatenschutzgesetz unterschiedliche Begrifflichkeiten verwendet. Während in der Datenschutzrichtlinie die „Verarbeitung“ (im weiteren Sinne) der Daten als Oberbegriff für jeden Vorgang im Zusammenhang mit den personenbezogenen Daten zu verstehen ist (Artikel 2 Buchstabe b DSRL), unterscheidet das Bundesdatenschutzgesetz zwischen den einzelnen Vorgängen der Erhebung, Verarbeitung (im engeren Sinne) und (sonstigen) Nutzung der Daten (§ 4 Absatz 1 BDSG). Materiell erfasst sind vor allem die Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung und Löschung von personenbezogenen Daten. Dabei ist ein technikneutrales Verständnis zugrunde zu legen. Erfasst sind sowohl automatische als auch nicht automatische Verfahren.[126]

Für einen kleinen Ausschnitt der personenbezogenen Daten gilt, in Anpassung an die Vorgaben der Datenschutzrichtlinie, ein erhöhtes Schutzniveau: Hierzu gehören die so genannten sensiblen Daten wie rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit und Daten über die Gesundheit und die Sexualität (vergleiche Artikel 8 DSRL, § 3 Absatz 9 BDSG).

In der digitalen Welt wirft das Kriterium des Personenbezugs allerdings zunehmend Probleme auf. Durch die Möglichkeit, Daten aller Art in einem bislang nicht dagewesenen Ausmaß miteinander zu verknüpfen, kann quasi jedes Datum zu einem personenbezogenen werden.

Persönlichkeitsrechtlich problematisch erscheint zunehmend weniger der Personenbezug an sich als vielmehr die Möglichkeit, jederzeit unterschiedlichste Daten aller Art

[121] Vgl. Kapitel 1.2.2, Beschlüsse des Düsseldorfer Kreises online abrufbar unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/index.php

[122] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 100.

[123] Vgl. Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 40.

[124] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 101.

[125] BVerfGE 65, 1, 45 – Volkszählung.

[126] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 49.

mit einzelnen Personen zu verknüpfen und in unterschiedlicher Weise auszuwerten. Geodaten, die an sich keine personenbezogenen Daten sind, jedoch schon immer personenbeziehbar waren, werden offensichtlich von vielen Menschen als problematisch im persönlichkeitsrechtlichen Sinne empfunden, wenn bestimmte technische Möglichkeiten der Verknüpfung und gezielten Recherche bestehen. Angesichts solcher Entwicklungen greift die Frage, ob Geodaten personenbezogene oder auch nur personenbeziehbare Daten sind, zu kurz.[127]

2.1.2 Grundprinzipien des Datenschutzrechts

Erlaubnisvorbehalt

Ein zentraler Grundsatz des Datenschutzrechts lässt sich in einem Satz wie folgt formulieren: Der Umgang mit personenbezogenen Daten ist verboten, es sei denn, der Betroffene willigt ein oder eine Rechtsnorm legitimiert ihn. Dieser Grundsatz ist sowohl im Gemeinschaftsrecht (Artikel 7 DSRL), als auch im nationalen allgemeinen (§ 4 Absatz 1 BDSG) und bereichsspezifischen Datenschutzrecht (zum Beispiel § 12 TMG) normiert. Demnach bestimmt sich die Zulässigkeit eines jeden einzelnen Datenverarbeitungsvorgangs danach, ob der Betroffene den Vorgang erlaubt hat oder ob dieser sich auf einen gesetzlichen Erlaubnistatbestand stützen lässt.[128]

Die Einwilligung ist vor allem im nicht-öffentlichen Bereich, neben den vertraglichen Legitimationen, von erheblicher Bedeutung.[129] Sie legitimiert einen Datenverarbeitungsvorgang nur dann, wenn sie wirksam erteilt wurde, wofür das Gesetz bestimmte Mindestanforderungen vorsieht (vergleiche § 4a BDSG oder auch Artikel 7 Buchstabe a DSRL). Nach nationalem Recht (§ 4a BDSG) ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruht, also ohne Zwang erfolgt. Dies setzt voraus, dass der Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann.

Die Einwilligung in die Datenerhebung oder -verarbeitung ist daher nur dann zulässig, wenn die betreffende Person „ohne jeden Zweifel ihre Einwilligung gegeben“[130] hat. Dies impliziert, dass die Einwilligung informiert, aktiv und freiwillig zu geschehen hat. Eine informierte Einwilligung setzt Transparenz und Kenntnis voraus. Allein durch die Nutzung einer Webseite kann keine aktive Einwilligung erteilt werden. Auch das Beibehalten von Einstellungen von Internetdiensten oder Browsern, die in der Voreinstellung nicht Privacy by Default[131] vorsehen, genügt nicht der Fiktion einer aktiven Einwilligung. Hier wird die Kenntnis der möglichen Einstellungen und ihrer Veränderungsmöglichkeiten vorausgesetzt, die jedoch weder bei jeder Nutzerin oder jedem Nutzer gleichermaßen gegeben ist noch von allen Diensteanbietern gefördert wird.

An der Möglichkeit zu einer freien Entscheidung kann es fehlen, wenn die Einwilligung in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird oder wenn der Betroffene durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wird.

Es gibt Situationen, in denen sich die Vertragspartner unterschiedlich stark gegenüberstehen. Für diese Fälle wird diskutiert, inwieweit eine freiwillige Einwilligung in die Datenerhebung vorliegt, insbesondere wenn Daten erhoben werden, die für die Erbringung der Dienstleistung selbst nicht benötigt werden. Für die Freiwilligkeit kann aber auch von Bedeutung sein, ob ein anderes Angebot in zumutbarer Weise zur Verfügung steht.[132]

Außerdem müssen die Betroffenen nach § 4a BDSG auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen werden. Wenn die Situation es erfordert oder die Betroffenen es verlangen, müssen diese auch darüber informiert werden, welche Folgen eine Verweigerung der Einwilligung nach sich zieht. Das geltende Recht lässt für das Internet die Möglichkeit einer elektronischen Einwilligung zu (§ 13 Absatz 2 TMG), die zum Beispiel durch Ankreuzen einer Checkbox erteilt werden kann.

Nach datenschutzrechtlichen Grundsätzen ist eine Einwilligung also nur dann wirksam, wenn sie in Kenntnis der entscheidungsrelevanten Umstände erteilt wird. Der Betroffene muss auf der Grundlage der ihm vorliegenden Informationen Bedeutung und Tragweite seiner Entscheidung zur Datenfreigabe erkennen können. Im Hinblick auf die spezifischen Bedingungen im digitalen Bereich ergeben sich hier neue Herausforderungen.

Die Frage von Transparenz- und Informationspflichten stellt sich in besonderem Maße. Auch Art und Weise der Informationspraxis sind bestimmend dafür, in welchem Umfang Bürgerinnen und Bürger bei Erteilung ihrer Einwilligung einschätzen können, welche Daten zu welchem Zweck gespeichert werden sollen.

Die Einwilligung kann bislang in unterschiedlicher Form eingeholt werden (Opt-in und Opt-out sowie unterschiedliche Formulierungen). Dies erfordert eine besondere Aufmerksamkeit und ein erhöhtes Textverständnis der in der Regel in juristischer Sprache formulierten Textpassagen. Eine informierte Einwilligung aufgrund dieser, der Absicherung eines Unternehmens dienenden Texte, ist aufgrund der Art des Textes und der gegebenen Informationen daher für viele Menschen nur schwer möglich. Gerade in der digitalen Welt gäbe es aber auch alternative Formen, Informationen verständlich bereitzustellen.

[127] Die Fraktion BÜNDNIS 90/DIE GRÜNEN hat gegen die Textfassung dieses Absatzes gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.1.1). Die Fraktion DIE LINKE. schließt sich diesem Sondervotum an.

[128] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 130 f.

[129] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 131.

[130] Vgl. Artikel 7 Buchstabe a DSRL.

[131] Vgl. hierzu Kapitel 2.3.5.

[132] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben gegen die Textfassung dieses Absatzes gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.1.2).

Einwilligungen werden unbefristet erteilt. Eine echte Transparenz und ein Überblick über die erteilten Einwilligungen ist für die Nutzerinnen und Nutzer angesichts der Vielzahl der eingeforderten Einwilligungen nur schwer zu behalten. Der Betreiber des Dienstes unterscheidet sich oftmals von der datenverarbeitenden Stelle; eine Transparenz darüber, welche Dienste beziehungsweise Unternehmen welche Daten erhalten, ist oftmals nicht vorhanden. In einer solchen Situation können Arbeitnehmer, Bürger und Nutzer ihre Informations-, Widerrufs-, Korrektur- und Löschrechte nur unzureichend geltend machen. Eine autonome Entscheidung über die Preisgabe eigener Daten im Internet können Menschen dann fällen, wenn sie Vor- und Nachteile ihrer Einwilligung einschätzen und Handlungsalternativen erkennen können. Die Medienkompetenz des Einzelnen trägt wesentlich dazu bei, informierte Einwilligungen zu ermöglichen und zu befördern. Diese kann aber nicht in gleicher Ausprägung von allen Personen erwartet werden und kann nicht als Ersatz für bedürfnisgerechtere Anforderungen an Transparenz, Information und Einwilligung stehen.

Im öffentlichen Bereich erfolgt die Datenverarbeitung personenbezogener Daten dagegen fast ausschließlich auf der Grundlage gesetzlicher Erlaubnistatbestände, die den verfassungsrechtlichen Anforderungen genügen müssen.

Die erfolgreichen Verfassungsbeschwerden der letzten Jahre zeigen allerdings, dass die verfassungsrechtlichen Vorgaben bei der Gesetzgebung teilweise nicht eingehalten wurden.[133]

Erforderlichkeitsgrundsatz

Der Erforderlichkeitsgrundsatz folgt aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz und ist zudem in Artikel 7 Buchstabe b bis f DSRL festgeschrieben. Er steht in engem Zusammenhang mit dem Grundsatz der Zweckfestlegung und der Zweckbindung. Demnach ist der Umgang mit personenbezogenen Daten auf das zum Erreichen des angestrebten Zieles erforderliche Minimum zu beschränken.[134] Es sollen nur so viele Daten erhoben, verarbeitet oder genutzt werden, wie zur Zweckerreichung unbedingt notwendig. Für den öffentlichen Bereich ist der Grundsatz in §§ 13 bis 16 BDSG (insbesondere in dem jeweiligen Absatz 1) normiert, wobei der zulässige Zweck auf die öffentliche Aufgabenerfüllung begrenzt ist. Der Erforderlichkeitsgrundsatz gilt aber auch im nicht-öffentlichen Bereich, wo seine effektive Verwirklichung durch eine möglichst genaue Zweckbestimmung bedingt ist.[135]

Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz besagt, dass die Daten, die für einen bestimmten Zweck erhoben worden sind, auch nur zu diesem Zweck verarbeitet oder genutzt werden dürfen.[136] Der Zweck der Datenerhebung begrenzt folglich den weiteren Umgang mit den erhobenen Daten. Sie dürfen nur zu dem Zweck weiterverwendet werden, der von der Einwilligung oder der konkret legitimierenden Rechtsnorm erfasst ist. Das setzt voraus, dass das Ziel der Datenverarbeitung oder -nutzung bereits vor der Datenerhebung so genau wie möglich bestimmt ist. Eine Speicherung auf Vorrat für künftige, noch nicht bekannte Zwecke ist dagegen grundsätzlich unzulässig.[137]

Vor allem im nicht-öffentlichen Bereich stößt die Beibehaltung dieses Grundsatzes auf praktische Probleme. In einer vernetzten Welt ist der Datenaustausch oftmals durch Spontanität und gerade nicht durch eine vorherige Festlegung des Verarbeitungszweckes bestimmt.[138] [139]

Transparenzgrundsatz

Die informationelle Selbstbestimmung setzt nach Auffassung des Bundesverfassungsgerichts voraus, dass Bürger wissen und grundsätzlich auch entscheiden können sollen, „wer was wann und bei welcher Gelegenheit“ über sie weiß.[140] Das setzt wiederum voraus, dass Datenerhebungs-, Datenverarbeitungs- und -nutzungsvorgänge transparent gestaltet werden. Zudem ist der Transparenzgrundsatz die grundlegende Voraussetzung dafür, dass Betroffene aktiv Datenschutzrechte wahrnehmen können. Transparenz wird in erster Linie durch den Grundsatz der Direkterhebung verwirklicht, wonach die Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4 Absatz 2 Satz 1, Absatz 3 BDSG), sodass er unmittelbar Kenntnis von dem Vorgang erlangt. Nur unter engen Voraussetzungen darf die Datenerhebung ohne Mitwirkung der Betroffenen erfolgen (§ 4 Absatz 2 Satz 2 BDSG). Flankiert wird das Transparenzgebot durch Auskunftsrechte sowie Informations-, Benachrichtigungs-, Unterrichtungs-, Hinweis- und Aufklärungspflichten der verantwortlichen Stelle.[141]

Gerade im nicht-öffentlichen Bereich wissen oftmals viele Bürgerinnen und Bürger nicht, wer eigentlich welche ihrer Daten zu welchen Zwecken speichert und verwendet.

Prinzip der Datenvermeidung und Datensparsamkeit

Der Grundsatz der Datenvermeidung und Datensparsamkeit ist – obwohl nicht durch die Datenschutzrichtlinie

[133] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel *Erlaubnisvorbehalt* abgegeben (siehe Kapitel 4.1.1.3).

[134] BVerfGE 65, 1, 46 – Volkszählung.

[135] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 136.

[136] Vgl, Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 48.

[137] Vgl. Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 48.

[138] Vgl. Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung. Die Verwaltung 2007, 153 (159).

[139] Die Fraktion DIE LINKE. hat gegen die Textfassung dieses Absatzes gestimmt und folgendes Sondervotum abgegeben: „DIE LINKE. trägt diesen Absatz nicht mit, da sie den Zweckbindungsgrundsatz für erhaltenswert hält. Sie ist zudem der Ansicht, dass Unternehmen Daten nicht spontan, sondern kommerziell speichern.“

[140] BVerfGE 65, 1, 43 – Volkszählung.

[141] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 136.

vorgegeben – in § 3a BDSG normiert. Er besagt, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen und auch die Datenverarbeitungssysteme an diesem Ziel auszurichten sind. Dabei handelt es sich um eine Konkretisierung des Erforderlichkeitsgrundsatzes auf technischer Ebene: Schon durch die entsprechende Technikgestaltung soll das Recht auf informationelle Selbstbestimmung präventiv geschützt werden.[142] Da der Grundsatz nicht sanktionsbewehrt ist, ist er – obwohl als Rechtspflicht formuliert – eher als Programmsatz zu verstehen.[143] [144]

2.1.3 Datenschutz im Grundgesetz

Verfassungsrechtliche Verortung

Der Grundrechtekatalog des Grundgesetzes enthält im Gegensatz zur Grundrechtecharta der Europäischen Union kein explizites Grundrecht des Datenschutzes.[145] Gleichwohl ist der Datenschutz ein Wert von Verfassungsrang und nimmt über verschiedene Grundrechte am Grundrechtsschutz teil. Namentlich finden sich datenschutzrechtliche Gehalte im allgemeinen Persönlichkeitsrecht (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG), im Brief-, Post- und Fernmeldegeheimnis (Artikel 10 GG) und im Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 GG). Als vorläufiger Höhepunkt in der Judikatur des verfassungsrechtlichen Datenschutzes wird das „IT-Grundrecht" auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme angesehen.[146]

IT-Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Als besondere Ausprägung des allgemeinen Persönlichkeitsrechts hat das Bundesverfassungsgericht im Hinblick auf Onlinedurchsuchungen das so genannte IT- beziehungsweise Computergrundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt.[147] Es „schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Artikel 10 oder Artikel 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist."[148] Der Schutz des Artikel 10 Absatz 1 Var. 3 GG versagt, wenn der Kommunikationsvorgang beendet ist oder der Zugriff außerhalb eines laufenden Kommunikationsvorgangs des Betroffenen erfolgt, was bei der Infiltration eines Computers regelmäßig der Fall ist.[149] Artikel 13 GG bietet raumbezogenen Schutz, welcher „nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren", da der Eingriff standortunabhängig über das Internet erfolgen kann.[150] Das Recht auf informationelle Selbstbestimmung trägt „den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potenziell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus."[151]

Erfasst sind Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten", wie zum Beispiel bei Personalcomputern oder Mobiltelefonen und elektronischen Terminkalendern, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.[152] Geschützt wird nicht nur vor einer Verletzung der Vertraulichkeit dieser Daten, sondern bereits vor dem Antasten der Integrität des Systems, da hierdurch „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen" ist.[153]

Dabei betont das Bundesverfassungsgericht, dass „der Standort des Systems […] ohne Belang und oftmals für die Behörde nicht einmal erkennbar" sei, was „insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone" gelte.[154] Daraus lässt sich schließen, dass der Schutz unabhängig davon zu gewährleisten ist, wo der Datenbestand gespeichert wird.

Die Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung erfolgt in erster Linie nach quantitativen Gesichtspunkten. Während das Grundrecht auf informationelle Selbstbestimmung Schutz vor Zugriff auf einzelne personenbezogene Daten gewährt, geht es beim (IT-)Grundrecht auf Gewährleistung der Vertraulichkeit

---

[142] Vgl. Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 3a Rn. 1.
[143] Vgl. Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 3a Rn. 2.
[144] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel *Prinzip der Datenvermeidung und Datensparsamkeit* abgegeben (siehe Kapitel 4.1.1.4).
[145] Vgl. zur Forderung eines Grundrechtes auf Datenschutz Kloepfer, Michael/Schärdel, Florian: Grundrechte für die Informationsgesellschaft – Datenschutz und Informationszugangsfreiheit ins Grundgesetz? JZ 2009, 453 ff. sowie unter 2.2.2.
[146] Vgl. Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1036).
[147] BVerfGE 120, 274, 302 ff. – Onlinedurchsuchung.
[148] BVerfGE 120, 274, 302 – Onlinedurchsuchung.
[149] BVerfGE 120, 274, 307 f. – Onlinedurchsuchung.
[150] BVerfGE 120, 274, 310 – Onlinedurchsuchung.
[151] BVerfGE 120, 274, 312 f. – Onlinedurchsuchung.
[152] BVerfGE 120, 274, 314 – Onlinedurchsuchung.
[153] BVerfGE 120, 274, 314 – Onlinedurchsuchung.
[154] BVerfGE 120, 274, 310 f. – Onlinedurchsuchung.

und Integrität informationstechnischer Systeme um den Schutz einer Vielzahl von (personenbezogenen) Daten (Datenbestand), die auf einem informationstechnischen System gespeichert sind. Denn wenn lediglich Daten mit einem punktuellen Bezug zu einem bestimmten Lebensbereich abgerufen werden, unterscheidet sich der staatliche Zugriff auf informationstechnische Systeme nicht von anderen Datenerhebungen und das Recht auf informationelle Selbstbestimmung ist anzuwenden.[155] Abgrenzungskriterium sind demnach Umfang und Vielfalt der Daten und das Ausmaß der durch die Daten zu gewinnenden Rückschlüsse auf die Person des Betroffenen. Ermöglicht die Datenerhebung potenziell eine umfassende Erkenntnisgewinnung über den Betroffenen, so ist das (IT-)Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschlägig.[156]

2.1.4 Das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts

Das allgemeine Persönlichkeitsrecht wird aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG hergeleitet. Es enthält mehrere Elemente und dient einerseits dem Schutz eines sozialen und räumlichen Rückzugsbereichs des Einzelnen und andererseits dem Schutz der individuellen Freiheit, selbst über die Präsentation der eigenen Person bestimmen zu können.[157]

Zur zweiten Gruppe gehören das Recht am eigenen Bild und am eigenen Wort und das seit dem Volkszählungsurteil aus dem Jahr 1983[158] verfassungsgerichtlich anerkannte Recht auf informationelle Selbstbestimmung. „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[159]

Informationelle Selbstbestimmung und Internet

Das Internet gibt den Menschen die Chance, selbstbestimmt und selbstbewusst ihr Leben zu gestalten. Innovative Nutzungsmöglichkeiten prägen den heutigen Alltag und stellen sich oft als Bereicherung oder praktische Hilfe dar. Die Möglichkeiten zur Information, Kommunikation und Interaktion werden erweitert.

Viele dieser Chancen und Möglichkeiten gehen mit der Speicherung, Verarbeitung und Übermittlung zahlreicher Daten einher. Voraussetzung für viele Informations- und Kommunikationsdienste sind personenbezogene Daten. Diese Dienste sind aber auch missbrauchsanfällig, sei es, dass mehr Daten als erforderlich gespeichert werden, sei es, dass Nichtberechtigte Zugang zu sensiblen Daten erlangen. Der Umgang mit personenbezogenen Daten hat sich im digitalen Zeitalter erheblich verändert. Im Kontext des Internets ist die Verarbeitung von personenbezogenen Daten vielfach ein wirtschaftliches Geschäftsmodell. Insbesondere in sozialen Netzwerken, aber auch bei anderen Diensten im Internet, werden eine Vielzahl von Daten von Nutzerinnen und Nutzern selbst zur Verfügung gestellt.

Durch die zunehmende Vernetzung, die Möglichkeit der Verknüpfung von personenbezogenen Daten (Persönlichkeitsprofile) und die ständige Weiterentwicklung automatischer Datenerfassungssysteme potenziert sich die Gefahr für das allgemeine Persönlichkeitsrecht in einer „Welt der allgegenwärtigen Datenverarbeitung"[160]. Diese Gefahr besteht nicht nur im Verhältnis der Bürger zum Staat, sondern auch im Verhältnis von Bürger zu Bürger und Verbrauchern zu Unternehmen untereinander. Dies zeigt sich besonders deutlich bei den Diensteanbietern im Internet. Der Erfolg von Google oder sozialen Netzwerken wie Facebook und studiVZ oder Internetprovidern ist geradezu dadurch bedingt, dass diese gigantische informationelle Infrastrukturen bereithalten.[161] Hier sind die Grundrechte zwar nicht (unmittelbar) anwendbar. Der Staat ist aber verpflichtet, „dem Einzelnen Schutz davor zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf die seine Individualität kennzeichnenden Daten nehmen"[162] (grundrechtliche Schutzpflicht). Schließlich hat die Verbreitung und Verarbeitung der eigenen personenbezogenen Daten im Internet mittlerweile die Grenzen der Nachvollziehbarkeit für den Einzelnen erreicht.

Der gegenwärtig diskutierte Datenschutz in sozialen Netzwerken wirft aber auch weitere Fragen auf. Diese betreffen insbesondere das Verhältnis der Nutzerinnen und Nutzer zu den Anbietern entsprechender Plattformen, beispielsweise wenn im Hintergrund personenbezogene Daten gesammelt und in Profilen zusammengeführt werden. Auch in diesem Fall muss der Schutz der informationellen Selbstbestimmung erhalten bleiben. Schließlich setzt die freie Entfaltung der Persönlichkeit auch voraus, dass der Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten geschützt wird.[163] Durch diese Schutzwirkung wird der abschreckende Effekt fremden (staatlichen und in Unternehmen vorhandenen) Geheimwissens gehemmt, „der entstehen und zur Beeinträchtigung bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß."[164] Mit anderen Worten: Wer befürchten muss, dass seine „Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, ver-

[155] BVerfGE 120, 274, 313 – Onlinedurchsuchung.
[156] Vgl. Hinz, Christian: Onlinedurchsuchungen. JURA 2009, 141 (144).
[157] Vgl. Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1036).
[158] BVerfGE 65, 1 – Volkszählung.
[159] BVerfGE 65, 1, 43 – Volkszählung.
[160] Zu diesem Begriff: Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung. Die Verwaltung 2007, 153 (155 ff.).
[161] Vgl. Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1039).
[162] BVerfG, Urteil vom 13. Februar 2007 – 1 BvR 421/05, BVerfGE 117, 202, 229 – Vaterschaftsfeststellung.
[163] BVerfGE 65, 1, 43 – Volkszählung.
[164] BVerfGE 113, 29, 46 – Beschlagnahme von Datenträgern.

wendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[165]

Mittlerweile hat sich daher ein kontextbezogener und gesetzlich zu gewährender Schutzrahmen mit unterschiedlichen Komponenten auf verschiedenen Ebenen herausgebildet. Dies reicht von gesetzlichen Regelungen im Bundesdatenschutzgesetz (wie beispielsweise dem bußgeldbewährten Kopplungsverbot des § 28 Absatz 3b BDSG), über die Auferlegung entsprechender Transparenz- und Informationspflichten für Betreiber von Diensten im Internet, bis hin zu einer Förderung der Medienkompetenz der Nutzerinnen und Nutzer für einen verantwortungsvollen Umgang mit den eigenen personenbezogenen Daten.[166]

2.1.5 Einschränkungen von Grundrechten/ Kollidierende Rechtsgüter

Gerade im Bereich des Internets sind zum Teil schwierige Grundrechtskollisionen vorgezeichnet, wie zum Beispiel die so genannte Spickmich-Entscheidung des Bundesgerichtshofs zeigt.[167] Pauschale Gegenüberstellungen etwa mit dem Eigentumsgrundrecht oder der Berufsausübungsfreiheit verbieten sich jedoch, da oft genug gefragt werden muss, ob bestimmte Grundrechtsausübungen zugleich den Schutz des Umgangs mit Daten von dritten Grundrechtsträgern umfassen. Hier ist eine besonders differenzierte Darstellung zu empfehlen.

Jedermann hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Dieses Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht 1983 in seiner Entscheidung zur Volkszählung, also im Hinblick auf eine staatliche Maßnahme, beschrieben hat, ist einerseits – als Ausprägung des allgemeinen Persönlichkeitsrechts aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG – ein individuelles Abwehrrecht gegenüber staatlichen Eingriffen.

Nach der Rechtsprechung des Bundesverfassungsgerichts wirkt sich das Recht auf informationelle Selbstbestimmung aber andererseits im Sinne einer Drittwirkung auch auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus und begründet staatliche Schutzpflichten. Die staatliche Gewalt ist danach verpflichtet, dem Einzelnen seine informationelle Selbstbestimmung im Verhältnis zu Dritten zu ermöglichen.[168] Gegebenenfalls müssen staatlicherseits die rechtlichen Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen kann.[169]

Nicht jede Beeinträchtigung eines grundrechtlichen Schutzbereichs führt per se zur Verfassungswidrigkeit der Maßnahme. Zum einen kann der Betroffene in die Maßnahme einwilligen und seine Daten freiwillig preisgeben, was vom Staat zu respektieren ist.[170] Aber auch ohne Einwilligung wird der verfassungsrechtliche Datenschutz nicht grenzenlos gewährleistet, sondern kann beschränkt werden. Das Bundesverfassungsgericht hat hierzu bereits 1983 im so genannten Volkszählungsurteil dargelegt: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung‘ sind nur im überwiegenden Allgemeininteresse zulässig.“[171]

Für diese Schrankenziehung hat das Bundesverfassungsgericht seit dem Volkszählungsurteil eine Reihe von Vorgaben aufgestellt, die es zu beachten gilt. Dabei gelten für die genannten Grundrechte weitgehend die gleichen Maßstäbe.[172]

Grundlegende Voraussetzung für einen zulässigen Eingriff in das Recht auf informationelle Selbstbestimmung ist das Vorhandensein einer gesetzlichen Grundlage, welche die Voraussetzungen und den Umfang der Beschränkungen klar erkennen lässt.[173] Das Erfordernis einer gesetzlichen Grundlage (Gesetzesvorbehalt) folgt bereits aus Artikel 2 Absatz 1 GG, wonach das allgemeine Persönlichkeitsrecht nur innerhalb der verfassungsmäßigen Ordnung gewährleistet wird. Die gesetzliche Grundlage muss dem Gebot der Normenklarheit entsprechen. Dies bedeutet, dass Anlass, Zweck und Grenzen eines Eingriffs in der Ermächtigung bereichsspezifisch, präzise und für die Bürgerinnen und Bürger klar erkennbar festgelegt werden müssen.[174]

Weiterhin muss der Verhältnismäßigkeitsgrundsatz beachtet werden. Das bedeutet, dass die Maßnahme einen legitimen Zweck verfolgen sowie zu dessen Erreichung geeignet, erforderlich und verhältnismäßig sein muss.[175] Der Zweck muss von vornherein bestimmt sein. Die ständige Rechtsprechung des Bundesverfassungsgerichts bringt deutlich zum Ausdruck, „dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu

[165] BVerfGE 65, 1, 43 – Volkszählung.
[166] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben gegen diese Textfassung des Kapitels *Informationelle Selbstbestimmung und Internet* gestimmt und ein Sondervotum abgegeben. Einem Teil dieses Sondervotums schließt sich die Fraktion BÜNDNIS 90/DIE GRÜNEN an (siehe Kapitel 4.1.1.5).
[167] BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328; vgl. auch Kapitel 1.3.5.
[168] BVerfG, Beschluss vom 23.Oktober 2006 – BvR 2027/02, Rn 30.
[169] BVerfG, Beschluss vom 23.Oktober 2006 – BvR 2027/02, Rn. 33.
[170] Vgl. BVerfG, Beschluss vom 23. Oktober 2006 – BvR 2027/02, Rn. 34; Schoch, Friedrich: Das Recht auf informationelle Selbstbestimmung. JURA 2008, 352 (357).
[171] BVerfGE 65, 1, 43 – Volkszählung.
[172] Vgl. BVerfGE, Beschluss vom 4. April 2006 – 1 BvR 518/0, BVerfGE 115, 320, 347 – Rasterfahndung II; Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1037 f.).
[173] BVerfGE 65, 1, 44 – Volkszählung.
[174] Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 79 m. w. N. aus der Rechtsprechung des BVerfG.
[175] BVerfGE 115, 320, 345 ff. – Rasterfahndung II.

unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist."[176]

Es besteht demnach ein „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten". Das Grundrecht auf informationelle Selbstbestimmung wird als besondere Ausprägung des schon zuvor grundrechtlich geschützten allgemeinen Persönlichkeitsrechts angesehen. Wie dieses wird es verfassungsrechtlich aus Artikel 2 Absatz 1 (so genannte allgemeine Handlungsfreiheit) in Verbindung mit Artikel 1 Absatz 1 GG (Menschenwürdegarantie) hergeleitet.

In der Verhältnismäßigkeitsprüfung findet eine Güterabwägung zwischen dem verfolgten Zweck und dem Recht auf informationelle Selbstbestimmung statt. Dabei ist von der Prämisse auszugehen, dass Grundrechte „jeweils nur soweit beschränkt werden dürfen, als es zum Schutze öffentlicher Interessen unerlässlich ist."[177] In der Abwägung ist vor allem das Gewicht der Grundrechtsbeeinträchtigung zu beachten. Bei der Beurteilung der Schwere des Eingriffs sind zum Beispiel die folgenden Kriterien zu berücksichtigen:

- in welche Sphäre die Maßnahme eingreift (Sozial-, Privat- oder Intimsphäre)[178]; die unterschiedliche Schutzintensität der drei Sphären kann aber nicht im Sinne eines starren Schemas verstanden werden, sondern nur als erster Orientierungspunkt für die Intensität der Grundrechtsbeeinträchtigung und für die Gewichtung der diese Beeinträchtigung rechtfertigenden Gründe,
- wie viele Grundrechtsträger betroffen sind,[179]
- wie intensiv die Beeinträchtigungen sind,[180]
- welche Inhalte von dem Eingriff erfasst werden, insbesondere welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen,[181]
- ob besondere Vertraulichkeitserwartungen verletzt werden,[182]
- auf welchem Weg die Inhalte erlangt werden,[183]
- welche weiteren Folgen oder Nachteile die Datenerhebung nach sich ziehen kann, zum Beispiel
  - das Risiko, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden,
  - eine stigmatisierende Wirkung,[184]
- die Heimlichkeit einer staatlichen Maßnahme, welche zum Beispiel die Möglichkeit der Inanspruchnahme von Rechtsschutz im Vergleich zur offenen Datenerhebung wesentlich erschwert,[185]
- der Verdachtsgrad,
- über welchen Zeitraum die Daten erhoben, verarbeitet und genutzt werden können und
- die Streubreite einer Maßnahme.

Zum zuletzt genannten Punkt hat das Bundesverfassungsgericht ausgeführt: „Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – weisen grundsätzlich eine hohe Eingriffsintensität auf. [...] Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. [...] Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen".[186]

Das Bundesverfassungsgericht hat eine anlasslose Speicherung von Telekommunikationsverkehrsdaten zwar nicht schlechthin als verfassungswidrig angesehen, aber betont, dass es sich um einen besonders schweren Eingriff handele, der höchsten verfassungsrechtlichen Anforderungen bei der Ausgestaltung der Regelungen unterliegt.

Je schwerer die Grundrechtsbeeinträchtigung wiegt, desto gewichtiger muss das staatliche Schutzgut sein, um den Eingriff rechtfertigen zu können. In die Waagschale gelegt werden können hier zum Beispiel:

- die Sicherheit des Staates als verfasste Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit,[187]
- die Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen Grundordnung,[188]

---

[176] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, NJW 2010, 833 (839 Rn. 213) – Vorratsdatenspeicherung.
[177] BVerfGE 65, 1, 44 – Volkszählung.
[178] In die Intimsphäre darf gar nicht eingegriffen werden, in die Privat- oder Geheimnissphäre nur unter besonders strenger Wahrung des Verhältnismäßigkeitsgrundsatzes und in die Sozialsphäre bereits nach den Kriterien, die für einen Eingriff in die allgemeine Handlungsfreiheit gelten. Vgl. Murswiek, Dietrich, in: Sachs, Michael (Hrsg.). Grundgesetz : Kommentar. 5. Auflage 2009, Artikel 2 Rn. 104 m.w.N.
[179] BVerfGE 115, 320, 347 – Rasterfahndung II.
[180] BVerfGE 115, 320, 347 – Rasterfahndung II.
[181] BVerfGE 115, 320, 348 – Rasterfahndung II.
[182] BVerfGE 115, 320, 348 – Rasterfahndung II.
[183] BVerfGE 115, 320, 348 – Rasterfahndung II.
[184] BVerfGE 115, 320, 351 ff. – Rasterfahndung II.
[185] Vgl. zum Beispiel BVerfGE 120, 274, 325 – Onlinedurchsuchung; BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06, BVerfGE 124, 43, 62 f. und 65 f. – Beschlagnahme von E-Mails.
[186] BVerfGE 115, 320, 354 f. – Rasterfahndung II.
[187] BVerfGE 120, 274, 319 und 328 – Onlinedurchsuchung.
[188] BVerfGE 115, 320, 358 – Rasterfahndung II.

– die Sicherung der Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen,[189]

– die Verhütung und Verfolgung von Straftaten von erheblicher Bedeutung[190] beziehungsweise schwerwiegender Straftaten.[191]

Eine absolute Grenze der Zulässigkeit einer Datenerhebung bildet die Schranken-Schranke des unantastbaren Kernbereichs privater Lebensgestaltung, insbesondere im Bereich der Intimsphäre. Staatliche Stellen „haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Artikel 1 Absatz 1GG ergibt. [...] Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen. [...] Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.“[192] Deshalb hat das Bundesverfassungsgericht als Voraussetzung für einen Zugriff auf einen Bereich, in dem solche Kernbereichsdaten (zum Beispiel tagebuchartige Aufzeichnungen, private Film- oder Tondokumente, höchstpersönliche Telefonate oder E-Mails) zu vermuten sind, das Erfordernis besonderer gesetzlicher Vorkehrungen aufgestellt, um den Kernbereich der privaten Lebensgestaltung zu schützen.[193] Zwar lässt sich die (beiläufige) Erfassung solcher Daten nicht immer verhindern. Jedoch sind entsprechende Maßnahmen abzubrechen, sobald erkannt wird, dass sie in den Kernbereich vordringen, oder zumindest im Nachhinein umgehend zu löschen.[194]

Aber auch unabhängig von diesem Kernbereich hat der Gesetzgeber „organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“[195] Dazu gehört auch die Sicherheit der Daten. So hat das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung vor allem die „gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit“ eingefordert.[196]

Im Falle des heimlichen Zugriffs auf die Datenverarbeitungsanlagen von Privatpersonen durch Sicherheitsbehörden (so genannte Onlinedurchsuchung) bestehen besonders hohe Hürden für den Gesetzgeber, die sich vorrangig aus dem neugeschaffenen Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ableiten. Onlinedurchsuchungen sind nur zulässig, wenn Gefahren für überragend wichtige Rechtsgüter bestehen, die sich in Gestalt von tatsächlichen Anhaltspunkten einer konkreten Gefahr manifestieren. Neben dem grundsätzlich geltenden Vorbehalt richterlicher Anordnung müssen unter anderem Vorkehrungen getroffen werden, die den Kernbereich privater Lebensgestaltung schützen.

2.1.6 Anonymität und Identitätsmanagement im Internet

Schwierige rechtliche Fragen wirft das vermehrt auch und gerade wegen des Internets geforderte Recht auf Anonymität auf. Gerade angesichts der zunehmend ubiquitären, alltäglich gewordenen digitalen Erfassung erscheint es als eine adäquate Antwort. Im Internet entfällt diese grundlegende Bedingung informationeller Freiheit häufig aus technischen Gründen. Der Gesetzgeber hat folgerichtig den Anbietern von Internetdiensten im Wirkungsbereich des Bundesdatenschutzgesetzes eine Rechtspflicht zur Anonymisierung beziehungsweise Pseudonymisierung bei der Ausgestaltung von Verfahren auferlegt (§ 3a BDSG). Für den Bereich der Telemediendienste hat er die Pflicht der Ermöglichung der anonymen beziehungsweise pseudonymen Nutzung von Telemedien und ihrer Bezahlung festgelegt (§ 13 Absatz 6 TMG).

Technische Möglichkeiten zur Anonymisierung helfen Nutzerinnen und Nutzern des Internets, ihr Recht auf informationelle Selbstbestimmung wirksam ausüben zu können. Sie sind daher auch weiterhin als ein Instrument des Selbstdatenschutzes zu fördern.

Die Wahrung der Anonymität gehört in der analogen Welt zu einem selbstbestimmten Leben. Diese Möglichkeit muss auch im Internet gegeben sein. Anders als in der analogen Welt fallen hier aber personenbezogene Daten systembedingt an. Die Erhebung und Verwendung muss dennoch auf ein Mindestmaß beschränkt werden.[197]

Mit dem Recht auf Anonymität geht auch die Möglichkeit eines selbstbestimmten Identitätsmanagements im Internet einher. Jedem Nutzer ist es selbst überlassen, wie viele und welche persönlichen Daten und Identitäten er in der digitalen Welt verwenden und preisgeben möchte. Dies schließt die Verwendung von Pseudonymen ausdrücklich ein.

Profilbildung kann Anonymität einschränken. Sie ist daher nur zulässig, wenn sie auf einer gesetzlichen Grundlage beruht (zum Beispiel Bundesdatenschutzgesetz oder Telemediengesetz). Der Begriff und die Konsequenzen einer Profilbildung sind allerdings noch nicht abschließend diskutiert und gesetzlich konkretisiert.[198]

---

189 BVerfGE 120, 274, 328 – Onlinedurchsuchung.
190 BVerfGE 113, 348, 385 – Vorbeugende Telekommunikationsüberwachung.
191 BVerfG, NJW 2010, 833, 848 Rn. 279 – Vorratsdatenspeicherung.
192 BVerfGE 120, 274, 335 – Onlinedurchsuchung.
193 BVerfGE 120, 274, 336 ff. – Onlinedurchsuchung.
194 BVerfGE 120, 274, 337 – Onlinedurchsuchung.
195 BVerfGE 65, 1, 44 – Volkszählung.
196 BVerfG, NJW 2010, 833, 840 Rn. 221 – Vorratsdatenspeicherung.
197 Die Fraktion DIE LINKE. hat ein ergänzendes Sondervotum zu diesem Absatz abgegeben (siehe Kapitel 4.1.1.6).
198 Die Fraktion DIE LINKE. hat gegen die Textfassung dieses Absatzes gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.1.7).

2.1.7 Sicherheit von Daten/Technischer Datenschutz

Die Entscheidungen des Bundesverfassungsgerichts zur Onlinedurchsuchung[199] sowie zur Vorratsdatenspeicherung[200] unterstreichen die gewachsene Bedeutung der Datensicherheit als einem wesentlichen Element des Datenschutzes.

Datensicherheit muss die mit der zunehmenden Vernetzung und Digitalisierung gewachsene Zugänglichkeit personenbezogener Daten und die damit verbundenen Risiken einfangen. Konzeptionell konzentriert sich die Diskussion auf präventiv angelegte und flexible Datensicherheitskonzepte unter Formulierung abstrakter Schutzziele.

Beim technischen Datenschutz ist auf eine technikneutrale Ausgestaltung von gesetzlichen Regelungen zu achten. Ein geeignetes Vorgehen kann hier die Formulierung von Schutzzielen darstellen, wie es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihren Eckpunkten für ein „Modernes Datenschutzrecht für das 21. Jahrhundert"[201] fordert.

Mit Privacy by Design und Privacy by Default können bereits die Hersteller von Hard- als auch Software verpflichtet werden, Produkte zu entwickeln, die über den gesamten Lebenszyklus hinweg zentralen Datenschutzprinzipien sowie den Zielen der Datensicherheit gerecht werden, nämlich:

- Vertraulichkeit,
- Integrität,
- Intervenierbarkeit,
- Verfügbarkeit,
- Transparenz,
- Möglichkeiten der Nichtverknüpfbarkeit.

Beispielsweise können mit Hilfe von Verschlüsselungstechniken, die dem Stand der Technik entsprechen, Kommunikationen als auch sensible Datenbestände abgesichert werden. Internetseiten könnten derart ausgestaltet werden, dass eine selbstbestimmte und informierte Entscheidung der Nutzerinnen und Nutzer bereits optimal in Design und Technik eingebettet erfolgt. Im Bereich des technischen Datenschutzes bestehen erhebliche Entwicklungsspielräume für den Schutz der Bürgerinnen und Bürger.

Den Datenschutzgesetzen würden so bei neuen technischen Entwicklungen nicht immer neue spezifische Regelungen hinzugefügt, sondern es müssten lediglich konkrete Maßnahmen für die Einhaltung des Datenschutzes spezifiziert werden. Aus übergeordneten Schutzzielen wären im Bedarfsfall gesetzliche Neuregelungen idealerweise ohne neue Grundsatzdiskussionen abzuleiten.

2.1.8 Selbstdatenschutz und Medienkompetenz

Die Stärkung allein des Datenschutzbewusstseins ist von der Stärkung der Medienkompetenz, zu der auch die Datenschutzkompetenz zu zählen wäre, zu unterscheiden. Nutzerinnen und Nutzer sind oft beim Umgang mit eigenen Daten nicht umsichtig genug. Weder erkennen sie, dass personenbezogene Daten anfallen, noch die Reichweite und die möglichen Folgen der Sammlung und Verarbeitung der angegebenen personenbezogenen Daten. Ohne diese Erkenntnis ist ein bewusster Umgang mit Daten aber nicht möglich.

Daher muss den Nutzerinnen und Nutzern sowohl das praktische und technische Verständnis für einen sorgfältigen Umgang mit den eigenen personenbezogenen Daten (zum Beispiel auch deren Schutz vor unerwünschtem Zugriff oder Weitergabe) als auch die Fähigkeit, mögliche Folgen und Konsequenzen der Nutzung entsprechender Angebote zu erkennen, vermittelt werden. Dies hilft nicht nur, datenschutzrechtliche Risiken für den Einzelnen zu minimieren, sondern eröffnet zugleich auch die Chance, sein Recht auf informationelle Selbstbestimmung bewusst auszuüben. Neben anderen Voraussetzungen ermöglicht die Kenntnis der Prozesse der Datenverarbeitung einen eigenverantwortlichen Umgang mit den Daten. Eine Stärkung des Selbstdatenschutzes kann eine Ergänzung zu, aber keinen Ersatz für gesetzliche Datenschutzregeln darstellen. Vor dem Hintergrund der Schwierigkeiten bei der Entwicklung international gültiger Datenschutzstandards gewinnt der Selbstdatenschutz auch weiter an Bedeutung.[202]

Die Vermittlung eines praktischen und rechtlichen Verständnisses muss daher eine gesamtgesellschaftliche Aufgabe sein.

2.1.9 Die Grenzen des nationalen Datenschutzes

Die Regeln der Datenerhebung und -verarbeitung bei Dienstleistungen, die sich an Bürgerinnen und Bürger der Europäischen Union wenden, bestimmen sich nach europäischem oder darüber hinausgehendem nationalen Recht. Die Datenschutzrichtlinie verbietet es grundsätzlich, personenbezogene Daten aus EU-Mitgliedstaaten in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Sie stellt allerdings eine Anzahl von Instrumenten zur Verfügung, die ein angemessenes Datenschutzniveau bei der Datenübermittlung in Drittstaaten sicherstellen sollen. Gegenwärtig erfolgt eine grundlegende Revision der Datenschutzricht-

[199] BVerfGE 120, 274 – Onlinedurchsuchung.
[200] BVerfG, NJW 2010, 833 – Vorratsdatenspeicherung.
[201] Vgl. hierzu auch Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 18 ff. http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile

[202] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben gegen die Textfassung dieses Absatzes gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.1.8).

linie, die auf Verbesserungen des Datenschutzes auch in diesem Bereich abzielt.

Die seit 2000 existierende Safe-Harbor-Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe-Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. In einem Beschluss vom April 2010 hat der Düsseldorfer Kreis die Anforderungen an die Nachweise und auch an deutsche Unternehmen, die an Nicht-EU-Unternehmen Daten übermitteln, verstärkt.[203]

Dem Grunde nach existieren Vorschriften, die europäische Bürger und Verbraucher schützen. Durch die offenbar mangelnde Durchsetzung der Sondervereinbarung mit den USA wurden diese Rechte allerdings geschwächt. Derzeit befindet sich die EU-Kommission (Generaldirektion Justiz) in Verhandlungen mit den USA über ein so genanntes Allgemeines Datenschutzabkommen, das neben Safe Harbor treten soll und insbesondere nach dem Inkrafttreten des Vertrags von Lissabon und der damit den EU-Institutionen zugewachsenen Mitzuständigkeit für Fragen der justiziellen und polizeilichen Zusammenarbeit von besonderer Bedeutung ist.

Ziel dieser Verhandlungen muss die Anwendbarkeit und Durchsetzbarkeit des europäischen Datenschutzrechts sein. Dabei wird unter anderem ein Geschäftssitz in Europa als Bedingung für die Erhebung und Verarbeitung von Daten diskutiert.

Gegenwärtig gilt nach dem Bundesdatenschutzgesetz das Sitzlandprinzip.[204] Danach kommt dasjenige Recht zur Anwendung, das am Sitz des für die Entscheidung über die Datenverarbeitung Verantwortlichen gilt. Damit wird ein harmonisierter EWR-Rechtsraum begründet. Eine Ausnahme bilden Verarbeitungen, bei denen noch eine Niederlassung im Inland besteht, sodass nationales Datenschutzrecht zur Anwendung kommt. Eine weitere Ausnahme vom Sitzlandprinzip bilden Verarbeitungen, bei denen Verantwortliche außerhalb des EWR-Raumes befindlich sind. So gilt beispielsweise mit Blick auf US-amerikanische Unternehmen das Territorialitätsprinzip und damit grundsätzlich bundesdeutsches Recht, sodass es auf den Ort der Datenverarbeitung beziehungsweise auf die Frage ankommt, ob sich automatisierte Mittel zur Datenerhebung räumlich gesehen in Deutschland befinden.

[203] „Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.“ (Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover, online abrufbar unter: http://www.bfdi.bund.de/cae/servlet/contentblob/1103868/publicationFile/88848/290410_SafeHarbor.pdf
Vgl. zur „Safe Harbor“-Vereinbarung auch Kapitel 1.2.2.

[204] § 1 Absatz 5 BDSG.

Genau diese Verräumlichung als Anknüpfungspunkt birgt mit Blick auf reine Webinhaltsangebote Probleme. So wird die Anwendbarkeit bundesdeutschen Rechts auf bestimmte Facebook-Bestandteile etwa dann bejaht, wenn es sich um eine Datenverarbeitung handelt, bei der ein so genannter Cookie auf dem privaten Rechner der Internetnutzer platziert wird, weil dieser im Inland gelegen ist. Für andere Angebote ohne Verwendung dieser Technologie hingegen wird – zumindest von Teilen der Aufsichtsbehörden – von einer fehlenden Anwendbarkeit mangels Inlandsbezuges der Datenverarbeitung ausgegangen. Die „Verhandlungen“ des Hamburgischen Datenschutzbeauftragten mit Google und Facebook sind nur vor diesem Hintergrund nachvollziehbar. Handelte es sich um einen unproblematischen Fall, wären verwaltungsrechtliche Anordnungen ergangen.

Auf europäischer und weltweiter Ebene muss die Bundesrepublik Deutschland ihrer Verantwortung als führender Wirtschaftsnation gerecht werden und für einen ausgeprägten Datenschutz streiten. Die Praxis global agierender Internetunternehmen erfordert ein abgestimmtes Vorgehen über die Grenzen des Nationalstaats hinaus. Bei internationalen Ausformulierungen von Datenschutzvorgaben sollte jeweils das höchste beteiligte Datenschutzniveau Grundlage sein.[205]

2.1.10 Datenschutz für Kinder und Jugendliche

Der Datenschutz bei besonders schutzwürdigen Gruppen bedarf besonderer Aufmerksamkeit. Die neuen informationstechnischen Möglichkeiten dürfen nicht zulasten der schwächsten Mitglieder unserer Gesellschaft (etwa von Kindern) gehen. Gleichzeitig sollen diese aber auch nicht von einer angemessenen Teilhabe an der Informationsgesellschaft ausgeschlossen sein.

Daten von Kindern werden in einem kaum geringeren Umfang als Daten von Erwachsenen erhoben und verarbeitet. Die Mehrzahl der Unternehmen unterscheidet hinsichtlich ihrer Internetangebote und der damit verknüpften Datenverarbeitungen nicht zwischen Erwachsenen und Kindern beziehungsweise Jugendlichen. Auch Kinder und Jugendliche sind aktive Nutzer von Informationsdiensten und setzen diese zum Informationsaustausch ein. Selbstverständlich sind dabei Kinder von Geburt an ebenso wie Erwachsene Träger von Grundrechten. Dazu gehört auch das Recht auf informationelle Selbstbestimmung, sodass auch Kinder und Jugendliche Datenschutzrechte und damit grundsätzlich das Recht haben, über die Herausgabe und Verwendung ihrer personenbezogenen Daten selbst zu bestimmen. Sie wachsen bereits mit der

[205] Die Fraktion DIE LINKE. hat zum Kapitel 2.1.9 *Die Grenzen des nationalen Datenschutz* folgendes Sondervotum abgegeben, das den von der Enquete-Kommission beschlossenen Text am Ende ergänzen soll: „Zudem darf die Tatsache, dass das nationale Datenschutzrecht zwar über EU-weit harmonisierte Regelungen hinausgehen kann, dann jedoch nur begrenzt anwendbar und durchsetzbar ist, nicht als Vorwand dafür missbraucht werden, eine Durchsetzung nationaler datenschutzrechtlicher Bestimmungen nicht zu forcieren. Unternehmen, die mit Angeboten auf dem deutschen Markt auftreten, müssen sich zwingend an hiesige Datenschutzvorschriften halten.“

Nutzung digitaler Technik und der Angebotsvielfalt des Internets auf und sind damit die am besten vernetzte Altersgruppe: 98 Prozent der Zehn- bis 18-Jährigen nutzen mittlerweile das Internet. Dies hat eine Studie (Jugend 2.0) im Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)[206] ergeben. Danach sind selbst Kinder im Alter von zehn bis zwölf Jahren zu 96 Prozent online. Hierbei überwiegen nach Angaben der Studie zwar die positiven Online-Erfahrungen, jedoch hat jeder dritte Jugendliche (34 Prozent) auch Negatives erlebt.

Die Studie zeigt weiterhin, dass das Internet für Jugendliche zwar eine herausragende Bedeutung hat, jedoch Freundschaften und Schule nicht verdrängt. Freunde, Familie und gute Noten sind wichtiger als das Netz. 98 Prozent der Jugendlichen sind ihre Freunde wichtig, 86 Prozent sagen dies vom Internetzugang. Die große Mehrheit der Zehn- bis 18-Jährigen verbringt mehr Zeit mit Freunden oder Hausaufgaben als im Internet. Die meisten Jugendlichen (76 Prozent) wissen bereits jetzt, das Internet sinnvoll zur Suche nach Informationen für Schule und Ausbildung einzusetzen. 64 Prozent haben nach eigenen Angaben so ihr Wissen verbessert, 38 Prozent ihre Leistungen in Schule oder Ausbildung.

Fast schon selbstverständlich ist für Teenager die Mitgliedschaft in Internetgemeinschaften. Nach der Studie sind 77 Prozent in so genannten Communitys angemeldet, 74 Prozent nutzen sie aktiv. Es gibt aber auch Unterschiede nach Altersgruppen: So sind 93 Prozent der 16- bis 18-Jährigen in den Netzwerken aktiv, aber nur 42 Prozent der Zehn- bis Zwölfjährigen.[207] SchülerVZ liegt insgesamt in den Altersgruppen vor Facebook. Teenager haben in ihrer jeweils meistgenutzten Community im Durchschnitt 133 Kontakte, davon 34 „gute Freunde“. Die BITKOM-Untersuchung zeigt, dass sich 58 Prozent der Zehn- bis 18-Jährigen mehr Datenschutz wünschen.

Da bereits mehr als drei Viertel aller deutschen Kinder und Jugendlichen in sozialen Netzwerken angemeldet sind und regelmäßig über diese Plattformen kommunizieren, entsteht teilweise bereits von jungen Teenagern ein genaues Persönlichkeitsprofil und ein digitales Abbild ihrer Wünsche, Vorlieben, Beziehungsgeflechte. Ihre Bedürfnisse werden ausgewertet.

Mit der gesellschaftlichen Debatte um die digitale Privatsphäre und Datenschutz in den letzten Jahren hat auch ein Erkenntnisprozess bei Kindern und Jugendlichen eingesetzt. Zunehmend werden schon Schulkindern die Probleme bewusst, die mit der Veröffentlichung von persönlichen Daten im Internet verbunden sein können. Sie überlegen sich bereits, was sie ins Netz stellen, ob sie ihren richtigen Namen verwenden etc. Auch Eltern erkennen die Gefahren des Internets für ihre Kinder in steigendem Maße.

Die Studie Jugend 2.0 untersucht spezielle Bedürfnisse von Kindern und Jugendlichen. Sie zeigt zudem, dass die Erfahrungen und das Wissen im Umgang mit Datenschutz und Persönlichkeitsrechten bereits mehrheitlich vorhanden sind, jedoch teilweise noch nicht in ausreichendem Maße. Bei Angeboten für Kinder und Jugendliche ist daher besonders auf eine altersgerechte Information und Aufklärung über die Datenerhebung, -verarbeitung sowie deren mögliche Konsequenzen zu achten. Nur so können Kinder und Jugendliche ihre Einwilligung in die Erhebung und Verarbeitung von personenbezogenen Daten überhaupt vornehmen. Dies ist unter anderem deshalb von besonderer Bedeutung, weil auch die Daten von Kindern und Jugendlichen bereits zu Profilen für gezielte Werbemaßnahmen zusammengefasst werden können. Kindern fällt es aber oftmals noch schwerer als Erwachsenen[208] zu erkennen, ob es sich um allgemeine oder aber speziell auf sie zugeschnittene Angebote handelt. Daher stellt sich letztlich auch die Frage, ob Kinder und Jugendliche, die nicht wie Erwachsene langfristige Folgen ihres Handelns abschätzen können, in stärkerem Maße einer öffentlichen Fürsorge und eines gesetzlichen Schutzes bedürfen.

Unterschiedliche Alterskategorien in verschiedenen Gesetzen erschweren eine Zuordnung. Bislang gilt, dass die gesetzlichen Vertreter des Kindes ihre Einwilligung in jede Verarbeitung der Daten des Kindes geben, bis das Kind selbst in der Lage ist, einzuwilligen. Die Einwilligungsfähigkeit des Kindes knüpft dabei an seine Einsichtsfähigkeit an, mit deren Zunahme sie graduell je nach der individuellen Entwicklung von den Eltern auf das Kind übergeht. Eine gesetzliche Vorgabe gibt es hierfür nicht.

Für Anbieter von Diensten ist das Alter des Nutzers oftmals nicht klar erkennbar. Dies gilt insbesondere bei der – aus Datenschutzgründen wünschenswerten – anonymen Nutzung von Diensten. Auch wechselnde Nutzer an einem Endgerät, wie es in Familien die Regel ist, erschweren eine klare Zuordnung zu bestimmten Altersklassen.

Deutliche Differenzierungen in den Schutzkonzepten erscheinen (wie zum Beispiel im Angebot beim sozialen Netzwerk SchülerVZ) wünschenswert, um einen verbesserten Schutz zu erreichen, wenn Angebote sich vollständig oder überwiegend an Jugendliche und Kinder wenden. Gegebenenfalls sind hier auch – entsprechend den jeweiligen Gefahren – gesetzgeberische Maßnahmen erforderlich. Unklarheiten der Auslegung des Bundesdatenschutzgesetzes hinsichtlich der Einwilligungsfähigkeit von Jugendlichen und der damit verbundenen Anforderungen an eine wirksame Einwilligung sollten beseitigt werden. Auch eine Begrenzung der zu erhebenden Daten

[206] BITKOM: Jugend 2.0, Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen. 2011, online abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Studie_Jugend_2.0.pdf

[207] Mädchen kommunizieren intensiver als Jungen. Das gilt nicht nur für Internet-Communitys, die von 82 Prozent der Mädchen aktiv genutzt werden, gegenüber 64 Prozent bei Jungen (BITKOM: Jugend 2.0 – Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen. 2011, S. 26, online abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Studie_Jugend_2.0.pdf)

[208] Vgl. hierzu Kapitel 2.3.1.2.

beziehungsweise eine nur eingeschränkte kommerzielle Verwertung käme diesbezüglich in Betracht.

Einer Altersverifikation, die zu einer eindeutigen Identifizierung des Nutzers führt, würde jedoch das Datenschutzrecht entgegenstehen. Denn diese hätte einen viel gravierenderen Eingriff zur Folge als das bisherige Fehlen datenschutzrechtlich hinreichend bedarfsgerecht zugeschnittener Angebote. [209]

2.2 Datenschutz im öffentlichen Bereich

2.2.1 Datenschutz in öffentlichen Einrichtungen

2.2.1.1 Einführung

Das deutsche Datenschutzrecht beruht seit seinen Anfängen auf einer Unterscheidung zwischen Datenschutz im Bereich öffentlicher Einrichtungen und nicht-öffentlicher Stellen, insbesondere in der Privatwirtschaft. Diese Differenzierung, die sich auch in der Struktur des Bundesdatenschutzgesetzes niedergeschlagen hat, findet ihren Ausgangspunkt in der Konzeption des Rechts auf informationelle Selbstbestimmung als einem individuellen Abwehrrecht gegenüber staatlichen Eingriffen. In diesem Zusammenhang wird darauf hingewiesen, dass die grundrechtlichen Grenzen für staatliche Datenverarbeitung enger sind als im nicht-öffentlichen Bereich. Die öffentliche Gewalt wird durch die Grundrechte verpflichtet und kann sich nicht auf eigene entgegenstehende Grundrechte berufen. Zwischen staatlichen und nicht staatlichen Gefährdungen der informationellen Selbstbestimmung besteht daher weiterhin ein Unterschied.[210] Die Datenschutzrichtlinie kennt diese Zweiteilung jedoch nicht. Das deutsche Recht sieht derzeit zumindest teilweise eine Gleichstellung öffentlicher und privater Datenverarbeitung vor, etwa für Telemedien.[211]

Da das Grundgesetz keine zentrale Kompetenznorm für die Gesetzgebung im Bereich des Datenschutzes enthält, ergibt sich die Zuständigkeit für die Gesetzgebung als Teil der Regelungskompetenz für das jeweilige Verwaltungsverfahren aus den Sachkompetenzen der Artikel 73 und 74 GG.[212] Bundesgesetze können daher den Datenschutz nur für Bereiche der Gesetzgebung des Bundes regeln. Entsprechendes gilt für Landesgesetze.

Neben der Unterscheidung datenschutzrechtlicher Bestimmungen für den privaten und öffentlichen Bereich ergibt sich also noch eine weitere Differenzierung zwischen bundes- und landesrechtlichen Normen. Dieses Nebeneinander bundes- und landesrechtlicher Vorschriften kennzeichnet besonders den öffentlichen Bereich, da im privaten Bereich im Rahmen der konkurrierenden Gesetzgebungskompetenz nach Artikel 74 Nummer 11 GG (Recht der Wirtschaft) viele Bereiche – einschließlich der jeweiligen datenschutzrechtlichen Aspekte – durch Bundesgesetze geregelt sind, sodass für den privaten Bereich wenig Regelungsmöglichkeiten für die Länder verbleiben.[213]

Darüber hinaus sind in vielen Fallkonstellationen Fragen der Spezialität und Subsidiarität von Normen zu beantworten. So haben etwa nach § 1 Absatz 3 BDSG andere datenschutzrechtliche Vorschriften des Bundes Vorrang vor dem Bundesdatenschutzgesetz. Vollziehen Landesbehörden Bundesrecht, gelten aufgrund einer weiteren Subsidiaritätsregelung (§ 1 Absatz 2 Nummer 2 BDSG) statt des Bundesdatenschutzgesetzes die Landesdatenschutzgesetze, dies jedoch nur, soweit das zu vollziehende Bundesrecht (zum Beispiel SGB, StVG) keine datenschutzrechtlichen Bestimmungen enthält.[214] Ganz überwiegend gilt auch für die Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen Regelungen.[215]

Vielfach wird daher ein unübersehbares „Dickicht des bereichsspezifischen Datenschutzes“[216] beklagt. Im Ergebnis hat dies dazu geführt, dass im Bereich öffentlicher Einrichtungen das Bundesdatenschutzgesetz nicht das zentrale Regelungsinstrument darstellt.[217]

Die deutliche Unterscheidung zwischen Datenschutz im öffentlichen und privaten Bereich gilt auch für die Organisation der Aufsicht und der Kontrollorgane. Während Bundes- und Landesdatenschutzbeauftragte die jeweilige Kontrolle über die Bundes- und Landesverwaltung ausüben, wird die Kontrolle im privaten Bereich ausschließlich auf Länderebene, teilweise durch die Landesdatenschutzbeauftragten, teilweise durch gesonderte Aufsichtsbehörden, ausgeübt. Gesonderte Kontrolleinrichtungen gibt es etwa im Bereich der Kirchen und öffentlich-rechtlicher Rundfunkanstalten.

Der Datenschutzaufsicht kommt für die Verwirklichung eines effizienten Datenschutzes eine herausragende Rolle zu. Eine Stärkung der Aufsichtsbehörden bedeutet somit zugleich eine Verbesserung des Datenschutzes. Vor dem Hintergrund der jüngsten Rechtsprechung des Europäischen Gerichtshofs[218] ist es zwingend notwendig, die völlige Unabhängigkeit der Datenschutzaufsicht zu gewährleisten. Durch die Entscheidung des Europäischen Gerichtshofs könnte auch ein gesetzgeberisches Handeln

[209] Die Fraktion DIE LINKE. sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben gegen diese Textfassung des Kapitels 2.1.10 *Datenschutz für Kinder und Jugendliche* gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.1.9).

[210] Vgl. auch Di Fabio, Udo, in : Maunz/Dürig, Grundgesetz - Kommentar. 58. Ergänzungslieferung 2010, Artikel 2, Rn. 190.

[211] Vgl. § 1 Absatz 1 Satz 2 TMG.

[212] Vgl. Kühling, Jürgen/Seidel, Christian/Siviridis, Anastasios: Datenschutzrecht. 2008, S. 74.

[213] Vgl. Kilian, Wolfgang/Weichert, Thilo, in: Kilian, Wolfgang/Heussen, Benno (Hrsg.), Computerrechts-Handbuch. 28. Ergänzungslieferung 2010, 1. Abschnitt, Teil 13, Punkt I., Rn. 3.

[214] Vgl. Bergmann, Lutz/Möhrle, Roland / Herb, Armin: Datenschutzrecht. Stand April 2010, Ziff. 3.3.2.2.

[215] Vgl. Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 1, Rn. 33.

[216] Bergmann, Lutz/Möhrle, Roland/Herb, Armin: Datenschutzrecht. Stand April 2010, Ziff. 4.1.2.

[217] Vgl. Bergmann, Lutz/Möhrle, Roland/Herb, Armin: Datenschutzrecht. Stand April 2010, Ziff. 3.2.7.

[218] EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland. Vgl. hierzu auch unter 1.2.3.

auf Bundesebene erforderlich sein. Ein entsprechender Auftrag zur Prüfung ist bereits durch die fraktionsübergreifende Entschließung des Deutschen Bundestages vom 16. Dezember 2010 erteilt worden.[219] Die Datenschutzrichtlinie gibt vor, dass die Datenschutzaufsicht rechtlich, organisatorisch und finanziell unabhängig sein muss. Hierbei unterscheidet die Richtlinie nicht zwischen öffentlichem und privatem Bereich.

2.2.1.2 Das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz[220] ist ein Schutzgesetz, das natürliche Personen schützen soll. Verstöße dagegen können Schadenersatzansprüche begründen. Allerdings begrenzt das Bundesdatenschutzgesetz die Möglichkeit einer verschuldensunabhängigen Haftung für Datenschutzverstöße auf die öffentlichen Einrichtungen (§§ 7, 8 BDSG).

Das Datenschutzgesetz ist daneben ein Eingriffsgesetz, mit dem Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gerechtfertigt werden. Die konkreten Eingriffsnormen beziehungsweise Eingriffe müssen durch ein überwiegendes Allgemeininteresse gerechtfertigt sein. Sie müssen zudem den Grundsätzen der Verhältnismäßigkeit und der Normenklarheit genügen sowie Schutzvorkehrungen zum Zwecke der Datensicherheit und der Sicherung der Betroffenenrechte vorsehen.

Nach dem Bundesdatenschutzgesetz gilt – wie im gesamten Datenschutzrecht – wegen des mit der Datenverarbeitung verbundenen Grundrechtseingriffs und dem Gesetzesvorbehalt das Verbot mit Erlaubnisvorbehalt (§ 4 Absatz 1 BDSG). Das heißt, Datenverarbeitung ist nur dann zulässig, wenn entweder eine Rechtsvorschrift dies ausdrücklich vorsieht oder der Betroffene ausdrücklich eingewilligt hat. Hierbei sind im Sinne der Rechtsprechung des BVerfG besonders hervorzuheben:

– die Zweckbindung für die Verwendung personenbezogener Daten,

– eine strikte Beschränkung der Datenverarbeitung und -nutzung auf das Erforderliche,

– die größtmögliche Selbstbestimmung der Betroffenen sowie

– die Transparenz der Datenverarbeitung.

Nur bei Beachtung dieser Anforderungen ist der notwendige Schutzzweck für ein modernes Datenschutzrecht gewährleistet.

Über das Bundesdatenschutzgesetz hinaus finden sich weitere Datenschutzregelungen mit Relevanz für den staatlichen Bereich in dem Bundespersonalvertretungsgesetz (BPersVG) sowie den jeweiligen Landespersonalvertretungsgesetzen, dem Betriebsverfassungsgesetz (BetrVG), den jeweiligen Landesvorschriften zum Datenschutz, den sozialrechtlichen Vorschriften (SGB), dem Telekommunikationsgesetz (TKG), dem Telemediengesetz (TMG) sowie in diversen EU- und UN-Richtlinien personenbezogene Daten betreffend.

Durch die engen Vorgaben zu Eingriffen in das Recht auf informationelle Selbstbestimmung wird dem Staat in Fragen des Datenschutzes eine Vorbildfunktion für nichtstaatliche Akteure zugeschrieben.[221]

Auch wenn es im staatlichen Bereich einige Spezifika bezüglich des Beschäftigtendatenschutzes gibt, wird an dieser Stelle nicht darauf eingegangen. Vielmehr ist das Thema Beschäftigtendatenschutz übergreifend, sowohl für den privaten als auch den öffentlichen Sektor, Gegenstand des Kapitels 2.3.

2.2.1.3 Staatliche Datenverarbeitung im Wandel

Die Anfänge der Datenschutzbewegung in Europa wie auch in den USA wandten sich gegen als übermächtig und bedrohlich empfundene Datenerhebungsprojekte staatlicher Stellen. Hinter diesen Projekten stand die zunehmende Computerisierung der Verwaltung, die neue Möglichkeiten einer Zusammenführung und Auswertung von personenbezogenen Daten erst ermöglichte. Die geplante Volkszählung zu Beginn der 1980er Jahre und das daraufhin 1983 ergangene Volkszählungsurteil des BVerfG[222] etablierten dann endgültig die bis dahin noch streitigen rechtlichen Grundprinzipien des Datenschutzes.

Nachfolgend haben Gesetzgeber und Verwaltung in der Verfolgung ihrer Aufgaben weiterhin Instrumente und Verfahren vorangetrieben, die zumindest mit Blick auf den Datenschutz erhebliche Probleme aufwiesen. Dies gilt in zunehmendem Maße auch für Vorhaben auf europäischer Ebene. Die Vielzahl an Entscheidungen des Bundesverfassungsgerichts zu Bundes- und Landesgesetzen (zum Beispiel G 10-Entscheidung[223], Großer Lauschangriff[224], Onlinedurchsuchung[225], Rasterfahndung[226], KFZ-Kennzeichenerfassung[227] sowie Vorratsdatenspeicherung[228]) markiert dabei einen aktuellen Stand des Datenschutzes im öffentlichen Bereich, der auf den Widerstreit zwischen den von staatlichen Stellen in Anschlag gebrachten öffentlichen Interessen einerseits sowie dem insbesondere vom Bundesverfassungsgericht betonten verfassungsrechtlichen Persönlichkeitsrecht andererseits hinweist.

Die Auseinandersetzung beschränkt sich dabei nicht auf den Sicherheitsbereich, sondern findet ihre Fortsetzung

[219] Bundestagsdrucksache 17/4179, S. 3.
[220] Vgl. auch Kapitel 1.3.2.

[221] Die Fraktion DIE LINKE. hat ein ergänzendes Sondervotum zu diesem Absatz abgegeben (siehe Kapitel 4.1.2.1).
[222] BVerfGE 65,1 – Volkszählung.
[223] Beschluss vom 20. Juni 1984 – 1 BvR 1494/78, BVerfGE 67, 157 – G 10.
[224] BVerfGE 109, 279 – Großer Lauschangriff.
[225] BVerfGE 120, 274 – Onlinedurchsuchung.
[226] BVerfGE 93, 181 – Rasterfahndung I; BVerfGE 115, 320, 345 ff. – Rasterfahndung II.
[227] BVerfG, Urteil vom 11. März 2008 – 1 BvR 2074/05 - KFZ-Kennzeichenerfassung, teilweise abgedruckt in MMR 2008, 308.
[228] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 – Vorratsdatenspeicherung.

auch in anderen Bereichen der öffentlichen Verwaltung, so etwa in den aktuellen Auseinandersetzungen um Grenzen zulässiger Datenerhebung bei Hartz-IV-Empfängern oder die Ausweitung staatlicher Kontodatenzugriffe.

2.2.1.4 Herausforderungen für das Datenschutzrecht in öffentlichen Einrichtungen

Die Informationsverarbeitung öffentlicher Stellen stellt besondere Herausforderungen an den Datenschutz, denn

– viele staatliche und kommunale Aufgaben – zum Beispiel in den Bereichen Steuerverwaltung, Justiz, Sicherheit, Sozialhilfe und Gesundheitswesen – erfordern naturgemäß die Erfassung und Verarbeitung personenbezogener Daten, die einen besonderen Schutzbedarf aufweisen können,

– die mit der Informationsverarbeitung einhergehenden Fachaufgaben, insbesondere in der Eingriffsverwaltung, sind gesetzlich legitimiert,

– die vollständige Durchdringung der öffentlichen Verwaltung mit IT hat zur Konsequenz, dass die öffentliche Verwaltung in ihrer Gesamtheit über ein fast lückenloses Datenprofil aller Bürgerinnen und Bürger verfügt.

Datenschutz im öffentlichen Bereich muss vor diesem Hintergrund sicherstellen, dass

– die Informationsverarbeitung und die damit verbundene Einschränkung des informationellen Selbstbestimmungsrechtes in jedem Anwendungsfall rechtlich legitimiert und angemessen ist (Erforderlichkeitsgrundsatz),

– die personenbezogenen Daten nur zu dem Zweck verwendet werden, für den sie erfasst wurden (Zweckbindungsgrundsatz),

– betroffene Bürger wissen, welche öffentlichen Stellen welche Daten über sie gespeichert haben (Transparenzgrundsatz), und

– nur solche personenbezogenen Daten von Bürgern erfasst und gespeichert werden, die zur Erledigung der jeweiligen Aufgabe unbedingt erforderlich sind (Datenvermeidungs- und Datensparsamkeitsgrundsatz).

Die bereichsspezifischen Regelungen zum Datenschutz sollen nicht nur einer materiellen Verletzung dieser Grundsätze vorbeugen, sondern darüber hinaus auch vermeiden, dass die persönlichen Grundrechte durch ein diffuses Gefühl totaler staatlicher Überwachung[229] eingeschränkt oder beeinträchtigt werden.

Gerade um diesem diffusen Gefühl totaler staatlicher Überwachung entgegenzutreten, wird diskutiert, ob und wie Auskunftsrechte für Bürgerinnen und Bürger und Auskunftspflichten staatlicher Stellen, etwa im Zusammenhang mit den Informationsfreiheitsgesetzen der Länder und des Bundes, überprüft und gegebenenfalls ausgebaut werden sollten.

Bei bisherigen Gesetzgebungsvorhaben konnten oft während des parlamentarischen Verfahrens noch Veränderungen hin zu einer Reduzierung der Menge an gesammelten personenbezogenen Daten erreicht werden, jedoch nicht ein vollständiger Verzicht auf das jeweilige Vorhaben. Gesetzliche Schutzprogramme für den Datenschutz können zudem vielfach mit der technischen Entwicklung nicht Schritt halten. Beim Betrieb bestehender oder der Einführung neuer IT-Infrastrukturen in öffentlichen Einrichtungen ergeben sich daher eine Vielzahl datenschutzrechtlicher Fragestellungen.[230]

Deren frühzeitige Einbeziehung in alle Projekte, unter anderem bei der Entwicklung der jeweiligen Hard- und Software, ist unabdingbar. Die Umstellung bestehender Verwaltungsverfahren auf elektronische Basis birgt dabei auch Chancen für den Datenschutz. Die zukünftige Technik kann bereits frühzeitig nach den Geboten der Datensparsamkeit und -sicherheit gestaltet werden.[231]

Fragen des Datenschutzes in öffentlichen Einrichtungen werden vielfach unter den Stichworten „E-Government und Datenschutz“ thematisiert. Als besondere Herausforderungen werden hierbei unter anderem beschrieben:[232]

– die Zunahme personenbezogener Daten, das heißt die gesamte Kommunikation Einzelner mit Behörden kann erfasst und analysiert werden; im Gegensatz dazu fallen etwa bei formlosen (fern-)mündlichen Anfragen bei einer Behörde üblicherweise keinerlei Daten an,[233]

– die Zunahme zentraler, bereichsübergreifender Datenbestände, etwa wenn Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer zentralen Stelle (etwa One-Stop-Government oder Lebenslagenkonzept) angeboten werden, beispielsweise durch den „einheitlichen Ansprechpartner“ nach der EU-Dienstleistungsrichtlinie, der als zentrale Anlaufstelle insbesondere für elektronische Behördendienste fungiert,[234]

– Fragen der Datensicherheit im Rahmen der elektronischen Kommunikation mit Bürgerinnen und Bürgern, etwa Gefährdungen des internen IT-Systems durch

[229] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, NJW 2010, 833 (839) – Vorratsdatenspeicherung.

[230] Die Fraktion DIE LINKE. hat gegen die Textfassung dieses Absatzes gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.2.2).

[231] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Bizer, Johann: eGovernment: Chance für den Datenschutz, online abrufbar unter: https://www.datenschutzzentrum.de/e-government/dud-200507.htm

[232] Vgl. Der Landesbeauftragte für den Datenschutz Niedersachsen: Herausforderungen für den Datenschutz bei eGovernment, online abrufbar unter: http://www.lfd.niedersachsen.de/live/live.php?navigation_id=13010&article_id=56234&_psmand=48

[233] Vgl. hierzu auch Yildirim, Nuriye: Datenschutz im Electronic Government. 2004, S. 64.

[234] Vgl. hierzu auch Petersen, Christin: Einheitlicher Ansprechpartner und Datenschutz. LKV 2010, 344 ff.

Systemöffnung oder die Notwendigkeit der Authentisierung bei Übermittlung personenbezogener Daten,

– Fragen der internen Datensicherheit,

– datenschutzrechtliche Verantwortlichkeiten bei Zusammenarbeit mehrerer Stellen, gegebenenfalls auch von Bund, Ländern und Kommunen,[235]

– die Einschaltung (privater) technischer Dienstleister.

2.2.1.5 Cloud-Computing in der öffentlichen Verwaltung

Cloud-Computing als Möglichkeit, Speicherkapazitäten, Rechenleistung und Software bedarfsspezifisch über das Internet zu beziehen, könnte perspektivisch auch in öffentlichen Einrichtungen an Bedeutung gewinnen. Die gemeinsame Nutzung von Hard- und Software sowie Rechenkapazitäten, die auf verschiedenen Servern nachfrage- und einzelfallabhängig zur Verfügung gestellt werden, könnte auch für Behörden, Ministerien und kommunale Selbstverwaltungskörperschaften möglicherweise Sparpotenziale durch Senkung der Ausgaben für eigene Hard- und Software eröffnen.[236]

Allerdings steht diese Form der Vernetzung behördlicher IT-Infrastrukturen, also der von unterschiedlichen Trägern der öffentlichen Verwaltung eingesetzten Hard- und Software, noch am Anfang.[237] Soweit ersichtlich, gibt es in Deutschland noch keine Nutzung von Cloud-Anwendungen durch öffentliche Stellen, wohl aber entsprechende Prüfungen.[238] Dabei wird davon ausgegangen, dass sich nur Modelle einer abgeschlossenen („privaten“) Cloud in alleiniger Verantwortung der öffentlichen Verwaltung als mögliche Option erweisen könnten.[239]

Daneben stehen andere Formen der Zusammenarbeit von öffentlichen Einrichtungen im IT-Bereich, etwa als Shared Service Center (SSC). Hierbei werden verwaltungsunterstützende Leistungen für die öffentliche Verwaltung zentral und gemeinschaftlich zur Verfügung gestellt. Interne Dienstleistungen (etwa Personalverwaltung oder Gebäudemanagement) werden also mittels gemeinsamer Nutzung von Ressourcen für mehrere Organisationseinheiten erbracht.[240]

Die Bundesregierung strebt an, die Entwicklung und Einführung von Cloud-Computing zu beschleunigen. Neben mittelständischen Unternehmen soll gerade der öffentliche Sektor frühzeitig von den Chancen profitieren. Unter anderem die Bereiche Sicherung und Schutz von Daten sind an die spezifischen Anforderungen von Cloud-Computing anzupassen. Datenschutz und Datensicherheit seien zwei der sich dabei ergebenden rechtlichen Herausforderungen.[241] Hierzu hat die Bundesregierung ein „Forschungsprogramm Sichere Internet-Dienste – Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)“ aufgelegt.[242]

Datenschutzrechtlich wird die Nutzung cloud-basierter Dienste bei der Verarbeitung personenbezogener Daten zumeist als Auftragsdatenverarbeitung im Sinne des § 11 BDSG eingeordnet. Verantwortlich für die Einhaltung datenschutzrechtlicher Vorschriften ist danach weiterhin der Auftraggeber (§ 11 Absatz 1 BDSG). Dieser ist insbesondere verpflichtet, den Gegenstand des Auftragsverhältnisses schriftlich hinsichtlich diverser Einzelaspekte genau festzulegen (etwa die nach § 9 BDSG zu treffenden technischen und organisatorischen Schutzmaßnahmen oder die Berechtigung zur Begründung von Unterauftragsverhältnissen). Diese rechtlichen Vorgaben setzen der cloudbasierten Verarbeitung personenbezogener Daten bisher enge Grenzen.[243] Im Übrigen gelten insoweit ähnliche Überlegungen wie für die datenschutzrechtliche Beurteilung von Cloud-Computing durch private Unternehmen.[244]

2.2.2 Mögliche Erweiterung des Grundgesetzes im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Der Schutz der informationellen Selbstbestimmung ist ebenso wie der Schutz der Vertraulichkeit der Kommunikation ein in vielen Landesverfassungen sowie internationalen Konventionen anerkanntes Grund- und Menschenrecht. Mit der europäischen Charta der Grundrechte wurde zudem ein Grundrecht auf Datenschutz geschaffen.[245] Das Grundgesetz enthält weder ein explizites

[235] Vgl. hierzu auch Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 15. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile

[236] Vgl. Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung. MMR 2010, 75 ff.

[237] Vgl. Schulz, Sönke: Cloud Computing in der öffentlichen Verwaltung. MMR 2010, 75 ff.

[238] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 12. Online abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/

[239] Vgl. Schulz, Sönke: Cloud Computing in der öffentlichen Verwaltung. MMR 2010, 75 (78).

[240] Vgl. Schulz, Sönke: Cloud Computing in der öffentlichen Verwaltung. MMR 2010, 75 (76).

[241] Bundesministerium für Wirtschaft und Technologie (Hrsg.): IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, online abrufbar unter: http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

[242] Bundesministerium für Wirtschaft und Technologie (Hrsg.): IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

[243] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 6.1., abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/; Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, 75 (78 f.). Zum Cloud-Computing vgl. auch Kapitel 2.3.3.

[244] Vgl. Schulz, Sönke: Cloud Computing in der öffentlichen Verwaltung, MMR 2010, 75 (78).

[245] Vgl. Artikel 8 GRC.

Grundrecht auf informationelle Selbstbestimmung noch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Bundesverfassungsgericht hat jedoch in Rechtsfortbildung[246] diese beiden Grundrechte – das Recht auf informationelle Selbstbestimmung und das Recht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme – aus den vorhandenen Artikel 1 Absatz 1 in Verbindung mit Artikel 2 Absatz 1 GG hergeleitet und angewendet.

Für eine ausdrückliche Aufnahme der beiden Grundrechte in die Verfassung wird vorgetragen, dass der Bedeutung der Entwicklung einer demokratischen und offenen digitalen Gesellschaft Rechnung getragen würde. Zudem hätte dies eine bessere Erkennbarkeit für den Bürger zur Folge. Mit der Aufnahme beider Grundrechte könnte auch der Verfassungsgesetzgeber die Rechtswirklichkeit an die veränderten Umstände in einer digitalen Gesellschaft anpassen, zumal das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in den kommenden Jahren noch weiter an Bedeutung gewinnen werden.

Eine entsprechende Ergänzung um das Grundrecht auf informationelle Selbstbestimmung sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme würde zudem die Übernahme des durch das Bundesverfassungsgericht beschrittenen Weges durch den Verfassungsgesetzgeber unterstreichen.

Gleichwohl fanden entsprechende Vorschläge für eine Verfassungsänderung im Deutschen Bundestag bisher keine Mehrheit.[247] Gegen die vorgeschlagenen Formulierungen wird vorgetragen, dass sie das Schutzniveau gegenüber der bestehenden Rechtslage senken könnten. Außerdem müsse sichergestellt sein, dass weiterhin Raum für eine künftige Auslegung des Grundgesetzes bleibe, sodass auf neue Fragen, die sich im Zusammenhang mit der technischen und gesellschaftlichen Entwicklung stellen, verfassungsrechtliche Antworten gefunden werden können.

2.2.3 Datensicherheit

Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme des öffentlichen Bereiches gegen unberechtigten Zugriff und missbräuchliche Nutzung von innen und außen geschützt sind. Die hierfür einschlägigen Schutzregelungen (z. B. Anlage zu § 9 BDSG) stammen aus einer Zeit, als Datenverarbeitung im öffentlichen Bereich durch Großrechner in abgeschotteten Rechenzentren gekennzeichnet war. Die jüngere Rechtsprechung[248] stellt in ihren Entscheidungen zunehmend auch auf die Bedeutung der informationstechnischen Sicherheit bei der Verarbeitung der personenbezogenen Daten ab.

Im Zuge des E-Government kommen längst Onlineverfahren zum Einsatz, bei denen Bürgerinnen und Bürger selbst auf die IT-Systeme der Verwaltung zugreifen. Durch diese Entwicklung und die fortschreitende Vernetzung der Verwaltungssysteme untereinander wird es zunehmend schwieriger, das technisch veraltete Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden.

Weitere Gesichtspunkte und Fragen der Datensicherheit werden zu einem späteren Zeitpunkt von der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission aufgegriffen.[249]

2.2.4 Datenschutzaudit und Gütesiegel zum Zwecke der Vertrauensbildung

Datenschutz in öffentlichen Einrichtungen (sowie bei nicht-öffentlichen Stellen) kann durch Auditierungsverfahren gefördert und erleichtert werden. Die Verleihung von Gütesiegeln sowie die Zertifizierung und Durchführung von Audit-Verfahren können wirkungsvolle, marktsteuernde Anreize für besseren Datenschutz geben. Ähnlich wie bei der technischen Betriebssicherheit (Technische Überwachungs-Vereine, TÜV) können Normen und Verfahren einen integrierten technischen Datenschutz fördern und gewährleisten. Die in den Bundesländern eingerichteten Datenschutzauditverfahren sowie das Europäische Datenschutz-Gütesiegel (EuroPriSe) können als praktische Beispiele hierfür angeführt werden.

Dabei wird das Datenschutzkonzept durch einen unabhängigen Gutachter förmlich geprüft und von einer unabhängigen öffentlichen Stelle bestätigt.

Im Unterscheid zu einer allgemeinen Beratung erfolgt beim Datenschutzaudit ein Mehr: Die Beratung bezieht sich auf die jeweils konkret vorgelegte Frage beziehungsweise auf den unterbreiteten Sachverhalt. Ob die gegebenen Empfehlungen umgesetzt werden, bleibt offen. Auch Veränderungen maßgeblicher Umstände werden nach Abschluss der Beratung nicht berücksichtigt. Das Audit hingegen ist auf eine dauerhafte Verbesserung der Datenschutzorganisation gerichtet. In Anlehnung daran könnte eine staatlich gestützte Datenschutzstiftung als Gütesiegelgarantie wirken und die Vertrauensbildung fördern.

2.3 Datenschutz im nicht-öffentlichen Bereich

2.3.1 Datennutzung als Bestandteil innovativer Dienste

Viele im Internet angebotene Dienste gehen aufgrund technischer Gegebenheiten mit einer Erhebung und Verarbeitung von Daten, in der Regel auch personenbezogener Daten, einher. Auf diese Art und Weise sind die Per-

[246] Vgl. zum Recht auf informationelle Selbstbestimmung: BVerfGE 65, 1, 45 – Volkszählung. Zum Recht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme vgl.: BVerfGE 120, 274 – Onlinedurchsuchung.

[247] Vgl. zuletzt Bundestagsdrucksache 16/9607 vom 18. Juni 2008 und Bundestagsdrucksache 16/13218 vom 27. Mai 2009.

[248] Vgl. BVerfG zur Online-Durchsuchung, BVerfGE vom 27. Februar 2008 – 1 BvR 370/07, NJW 2008, 822; sowie BVerfG zur Vorratsdatenspeicherung, Urteil vom 2. März 2010 – 1 BvR 256/08, BVerfGE 121, 1.

[249] Vgl. im Übrigen auch Kapitel 2.1.7.

sonalisierbarkeit und Interaktivität von Diensten im Internet realisierbar. Dienste können umso stärker an Interessen und Vorlieben ihrer Nutzerinnen und Nutzer angepasst werden, je mehr Daten über deren Verhalten verwertet werden. Auf diese Weise können die Anbieter auch möglichst passgenaue Werbung anbieten.

Strenge Datenschutzvorschriften können die Entwicklung neuer Anwendungen erschweren oder sie unbequemer in der Nutzung machen. Andererseits können strengere Vorschriften geeignet sein, Verbrauchervertrauen aufzubauen, was die Nutzerzahlen erhöhen kann.

Eine Missachtung der berechtigten Datenschutzerwartungen der Nutzerinnen und Nutzer kann auch zu einer Gegenreaktion und Ablehnung eines Dienstes führen. Letztlich setzen Geschäftsmodelle, die auf der Verwendung von personenbezogenen Daten beruhen, immer auch eine Akzeptanz des Nutzers voraus. Hieraus kann sich ein Selbstkorrektiv in der Entwicklung von Diensten ergeben, solange sichergestellt ist, dass die Nutzerinnen und Nutzer über Art und Umfang der vorgenommenen Datenverarbeitung informiert sind.

2.3.1.1 Datenschutz in der Informations- und Kommunikationsgesellschaft: Zum Spannungsverhältnis und Gebot der Abwägung zwischen Persönlichkeitsrechten und Kommunikationsgrundrechten

Dass das allgemeine Persönlichkeitsrecht mit der Meinungsfreiheit in Konflikt geraten kann, ist allgemein bekannt und Gegenstand des Äußerungsrechts. Die Berichterstattung durch die Medien (Presse und Rundfunk), aber auch die Wahrnehmung der Meinungsfreiheit durch den Einzelnen kann Persönlichkeitsrechte verletzen. Es handelt sich um das klassische Spannungsverhältnis zwischen Persönlichkeitsrechten und Meinungsfreiheit, und zwar unabhängig davon, ob die Meinungsfreiheit individuell vom Einzelnen oder durch Medien wahrgenommen wird.

In der Informations- und Kommunikationsordnung des Internets gewinnt dieses Spannungsverhältnis erheblich an Bedeutung. Dies liegt vor allem daran, dass der Einzelne im Internet ohne nennenswerte Zugangsschranken an der (Massen-)Kommunikation mitwirken kann. Die starren Grenzen zwischen Medien und Rezipienten verschwimmen.

Die moderne Internetkommunikation wirft eine Vielzahl von Fragen auf, die unter anderem die Zuordnung bestimmter Dienste zu den grundrechtlich geschützten Kommunikationsfreiheiten betreffen. Weil diese Zuordnungsfragen noch nicht geklärt sind, bereitet es oftmals Schwierigkeiten, die im Internet auftretenden Probleme als grundrechtliche Konflikte zwischen Persönlichkeitsgrundrechten und Kommunikationsgrundrechten wahrzunehmen. Recht einfach liegen die Dinge bei Blogs und sonstigen meinungsbildenden Portalen (Spickmich etc.), die sich aufgrund dieser meinungsbildenden Funktion im Schutzbereich der Kommunikationsgrundrechte bewegen. Es handelt sich letztlich um den klassischen Konflikt zwischen Meinungsäußerungsfreiheit und dem allgemeinen Persönlichkeitsrecht des Betroffenen.

Besondere Zuordnungsprobleme ergeben sich jedoch etwa bei solchen Diensten („Informationsintermediäre“), die im Gegensatz zu klassischen Medien Informationen nicht nach meinungsbezogenen, publizistischen Gesichtspunkten zusammenstellen und veröffentlichen, sondern nach „meinungsneutralen“ formalen Kriterien Informationen zusammentragen, speichern und verbreiten. So bereitet beispielsweise die rechtliche Einordnung von Suchmaschinen erhebliche Schwierigkeiten, auch wenn sich ihre Input-Funktion aus allgemein zugänglichen Quellen speist und die Benutzung von Suchmaschinen durch Nutzerinnen und Nutzer als Ausübung der grundrechtlich geschützten Informationsfreiheit (Artikel 5 Absatz 1 Satz 1 Alt. 2 GG, Artikel 10 Absatz 1 Satz 2 EMRK, Artikel 11 Absatz 1 Satz 2 GRC) zu qualifizieren ist. Ungeachtet dieser grundrechtlichen Zuordnungsprobleme steht in jedem Fall fest, dass solche Suchmaschinen aus der Informations- und Kommunikationsordnung des Internets nicht wegzudenken und für die Funktionsfähigkeit der modernen Informationsgesellschaft schlechthin unverzichtbar sind. Sofern solche Suchmaschinen personenbezogene Daten des Einzelnen zusammentragen, speichern und ein mehr oder weniger umfangreiches Persönlichkeits- oder Bewegungsprofil des Betroffenen auf Abruf zur Verfügung stellen, handelt es sich um einen Konflikt zwischen Kommunikationsgrundrechten und Persönlichkeitsrechten. Auch insoweit gilt es, durch Abwägung die einander widerstreitenden Güter im Sinne praktischer Konkordanz zu einem wechselseitig möglichst schonenden Ausgleich zu bringen.

Als weiteres Beispiel für die Schwierigkeiten, neue Internetdienste den klassischen Kommunikationsgrundrechten zuzuordnen, seien soziale Netzwerke genannt. Gleichwohl würde es die grundrechtliche Perspektive verengen, wenn man soziale Netzwerke ausschließlich aus dem Blickwinkel des verfassungsrechtlich geschuldeten Schutzes des Grundrechts auf informationelle Selbstbestimmung betrachtete.

Viele Nutzerinnen und Nutzer von sozialen Netzwerken und anderen Plattformen geben heute eine Vielzahl von Daten preis, darunter auch sensible Daten wie die religiöse oder politische Überzeugung und die sexuelle Orientierung. Die bewusste Verwendung und Offenbarung der eigenen Daten ist nicht pauschal zu kritisieren oder gar zu verurteilen. Sie ist vielmehr die Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung, also die Ausübung grundrechtlich geschützter Freiheit.

Ungeklärt ist, ob eine solche Preisgabe personenbezogener Daten darüber hinaus auch Ausdruck des Grundrechts der Meinungsfreiheit ist. In diesem Zusammenhang ist zunächst festzuhalten, dass jedenfalls die Veröffentlichung personenbezogener Daten in entsprechenden Datenbanken sozialer Netzwerke („Profile“ o. Ä.) sowie die nachgelagerte Kommunikation zwischen „Freunden“ oder sonstigen Teilnehmern des Kommunikationsnetz-

werkes auch der individuellen und öffentlichen Meinungsbildung dienen und daher kommunikationsgrundrechtlich geschützt sind. Für den Schutz oder die Werthaltigkeit der Kommunikationsordnung kommt es auf den privaten beziehungsweise nicht privaten Charakter der Informationen prinzipiell nicht an. Auch die Offenbarung privater Informationen dient dem Kommunikationsprozess. War die Berichterstattung über Privates (insbesondere von Prominenten) in der Vergangenheit regelmäßig den Medien vorbehalten, die sich insoweit auf die grundrechtlich geschützte Presse- beziehungsweise Rundfunkfreiheit berufen können[250], kann nunmehr der Einzelne im Internet Privates offenbaren. Diese Form der Freiheitsbetätigung beruht auf doppeltem Grundrechtsboden: Sie ist Ausdruck des Grundrechts auf informationelle Selbstbestimmung und zugleich Wahrnehmung der grundrechtlich geschützten Meinungsfreiheit. Der Schutz der Kommunikationsordnung ist umfassend und unteilbar. Er lässt sich nicht in schutzbedürftige, weniger schutzbedürftige oder schutzlose Informationen unterteilen. Dies gilt insbesondere unter den Bedingungen der modernen Internetkommunikation, in der – wie das Beispiel sozialer Netzwerke zeigt – die Grenze zwischen privaten und nicht privaten Informationen zunehmend verschwimmt.

Hieraus erhellt, dass die Veröffentlichung personenbezogener Daten in entsprechenden Datenbanken sozialer Netzwerke („Profile“ o. Ä.) als solche nicht nur Ausfluss des Grundrechts der informationellen Selbstbestimmung, sondern auch der Meinungsfreiheit ist. Zwar hat das Bundesverfassungsgericht in seinem Volkszählungsurteil die Verpflichtung zu Angaben im Rahmen statistischer Erhebungen nicht an der (negativen) Meinungsäußerungsfreiheit des Artikel 5 Absatz 1 Satz 1 GG gemessen, weil solche Angaben nicht durch Elemente der Stellungnahme, des Dafürhaltens und des Meinens gekennzeichnet sind.[251] Anders liegen die Dinge indes bei der Veröffentlichung personenbezogener Daten in sozialen Netzwerken. Zum einen beruhen solche Daten nicht nur auf „nackten“ Tatsachen, sondern oftmals auf persönlichen Einschätzungen, denen Wertungen zugrunde liegen (zum Beispiel: Selbsteinschätzung der politischen Überzeugung in sozialen Netzwerken, „Gefällt-mir“-Button).

Und zum anderen ist die Veröffentlichung von personenbezogenen Tatsachen, die für sich genommen keine „Meinungen“ sind, Voraussetzung für den Aufbau entsprechender Kommunikationsnetzwerke, in denen sich die grundrechtlich geschützte Kommunikation vollzieht. Wegen dieses engen funktionalen Zusammenhangs wird man die Veröffentlichung auch solcher Daten als Ausdruck der Meinungsäußerungsfreiheit qualifizieren können. Das gilt auch deshalb, weil die Preisgabe personenbezogener Daten im Rahmen der Kommunikation zwischen „Freunden“ oder sonstigen Teilnehmern des Kommunikationsnetzwerkes dem Schutz der Meinungsfreiheit unterfällt.

Eine pauschale Implementierung der datenschutzrechtlichen Grundsätze überall dort, wo grundrechtlich geschützte Kommunikationsinteressen betroffen sind, würde das verfassungsrechtliche Spannungsverhältnis zwischen dem grundrechtlich gebotenen Persönlichkeitsschutz einerseits und den Kommunikationsgrundrechten andererseits verfehlen. Von Verfassungs wegen gilt es, die einander widerstreitenden Güter im Sinne praktischer Konkordanz zu einem wechselseitig möglichst schonenden Ausgleich zu bringen.

Im Folgenden seien einige Abwägungsmaßstäbe genannt:

– Ob und in welchem Umfang der (volljährige) Einzelne personenbezogene Daten im Internet offenbart, ist prinzipiell seine Entscheidung. Der Staat hat kraft seiner ihm obliegenden Schutzpflichten allein – etwa durch Auferlegung entsprechender Transparenz- und Informationspflichten der Anbieter sozialer Netzwerke – dafür Sorge zu tragen, dass der Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann. Die grundrechtliche Schutzpflicht des Staates darf indes nicht in einen „Datenschutz vor sich selbst“ umschlagen. Nicht der Staat, sondern der Einzelne hat in Wahrnehmung seines Grundrechts auf informationelle Selbstbestimmung darüber zu entscheiden, ob und in welchem Umfang er personenbezogene Daten im Internet veröffentlicht und wem er diese öffentlich zugänglich macht (Prinzip der Eigenverantwortlichkeit). Im Rahmen der Abwägung ist dem möglicherweise ganz unterschiedlichen Schutzbedürfnis der verschiedenen betroffenen Personengruppen Rechnung zu tragen. Neben den individuellen Interessen des Einzelnen sind auch die Informationsinteressen der Allgemeinheit zu berücksichtigen. Alle diese Aspekte sind zu beachten, wenn der Gesetzgeber etwa vor der Entscheidung zwischen Opt-in- oder Opt-out-Regelungen steht.

– Letztlich muss der Einzelne autonom entscheiden, ob und in welchem Umfang und zu welchem Zweck er personenbezogene Daten in sozialen Netzwerken preisgibt und auf diese Weise nicht nur von seinem Grundrecht auf informationelle Selbstbestimmung, sondern auch von seinem Grundrecht der Meinungsfreiheit Gebrauch macht. Die Entscheidung über die Preisgabe personenbezogener Daten und über die Kommunikation mit anderen in sozialen Netzwerken obliegt allein dem Einzelnen. Die besondere Problematik besteht indes darin, dass es „den“ Nutzer nicht gibt. Um nur ein Beispiel zu nennen: Während der eine weniger Wert auf die Zweckbestimmung der erhobenen Daten legt, weil sich im Zeitpunkt der Informationspreisgabe die künftigen Verwendungszwecke noch nicht absehen lassen und weil er in der unterschiedlichen Verwendung seiner Daten gerade einen Vorteil sieht, ist für den anderen genau eine solche

[250] Deutlich zuletzt BVerfG, Beschluss vom 26. Februar 2008 – 1 BvR 1602, 1606, 1626/07, BVerfGE 120, 180, 205 – Caroline von Monaco III: „Der Schutzbereich der Pressefreiheit umfasst auch unterhaltende Beiträge über das Privat- oder Alltagsleben von Prominenten und ihres sozialen Umfelds, insbesondere der ihnen nahestehenden Personen.“ Siehe auch BVerfG, Urteil vom 9. November 1999 – 1 BvR 653/96, BVerfGE 101, 361, 389 ff. – Caroline von Monaco II.

[251] Vgl. BVerfGE 65, 1, 40 f. – Volkszählung.

exakte Zweckbestimmung unverzichtbar. Hier ergeben sich in regulatorischer Hinsicht erhebliche Probleme.

– Für die Lösung dieses Konflikts ist insbesondere von Bedeutung, mit welcher Intensität in das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird. Eingriffe in den Kernbereich des Grundrechts beziehungsweise in die Intimsphäre sind grundsätzlich unzulässig. Die Veröffentlichung von Daten aus dem Kernbereich privater Lebensgestaltung und Ehre oder der Intimsphäre und die Veröffentlichung aussagekräftiger Persönlichkeitsprofile durch einen Anderen sind schon zum Schutz der Menschenwürde generell unzulässig. Im Bereich der Privatsphäre wird zum Schutz des Grundrechts auf informationelle Selbstbestimmung regelmäßig eine ausdrückliche Zustimmung (Opt-in) erforderlich sein. Im äußeren Bereich der Sozialsphäre kann hingegen die Möglichkeit einer ausdrücklichen Ablehnung (Opt-out) ausreichend sein, um die Bedeutung der Kommunikationsfreiheit hinreichend zu berücksichtigen.

– Je mittelbarer der Personenbezug von Daten ist, desto weniger gewichtig ist das Recht auf informationelle Selbstbestimmung im Rahmen des erforderlichen Güterausgleichs. Weiter kommt es bei der Gewichtung darauf an, ob das Recht auf informationelle Selbstbestimmung in der Intim-, Privat- oder Sozialsphäre betroffen ist.

– Nicht nur unter den Bedingungen der modernen Informations- und Kommunikationsordnung muss sich die oder der Einzelne auch der Kontrolle und Kritik durch die Gesellschaft stellen. In ständiger Rechtsprechung weist das Bundesverfassungsgericht darauf hin, dass das allgemeine Persönlichkeitsrecht (im Bereich der Sozialsphäre) dem Träger keinen Anspruch darauf verleiht, nur so in der Öffentlichkeit dargestellt zu werden, wie er sich selber sieht oder gesehen werden möchte.[252] Die Grenzen zulässiger Berichterstattung sind erst bei schwerwiegenden Auswirkungen auf das Persönlichkeitsrecht überschritten, also dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu besorgen sind, wie es der Bundesgerichtshof kürzlich in der sogenannten Spickmich-Entscheidung nochmals klargestellt hat.[253]

– Sofern personenbezogene Daten aus allgemein zugänglichen Quellen (Internet o. Ä.) stammen und deshalb dem besonderen Schutz des Grundrechts der Informationsfreiheit (Artikel 5 Absatz 1 Satz 1 Alt. 2 GG, Artikel 10 Absatz 1 Satz 2 EMRK, Artikel 11 Absatz 1 Satz 2 GRC) unterfallen und nicht der Kernbereich des informationellen Selbstbestimmungsrechts beziehungsweise die Intimsphäre betroffen sind, ist die Erhebung, Speicherung und Verwendung personenbezogener Daten zulässig, es sei denn, dass das Betroffeneninteresse offensichtlich überwiegt. Dieses Wertungsmodell könnte als Leitprinzip für die Ausgestaltung künftiger Konfliktsituationen dienen.

Sofern der Einzelne in Kontakt oder Kommunikation mit anderen tritt (Sozialsphäre) und damit die persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt, muss er sich – im Interesse umfassender Kommunikation – Beschränkungen seines allgemeinen Persönlichkeitsrechts und seines Rechts auf informationelle Selbstbestimmung gefallen lassen. Insbesondere hat er keinen Anspruch darauf, in der Öffentlichkeit nur so dargestellt zu werden, wie er möchte.[254]

2.3.1.2 Geschäftsmodelle von Internetdiensten/ Onlinewerbung

Das Internet besteht sowohl aus Inhalten und Diensten, die allen Nutzerinnen und Nutzern kostenlos zur Verfügung stehen, als auch aus Inhalten und Diensten, die lediglich gegen Entgelt abgerufen werden können (Paid Content, Paid Services). Dabei ist die überwiegende Zahl der Inhalte derzeit entgeltfrei abrufbar. Viele dieser unmittelbar kostenfreien Inhalte und Dienste werden kommerziell erbracht, wobei Onlinewerbung nicht nur der Refinanzierung der Kosten dienen kann, sondern auch der Erzielung von Gewinnen. Aber auch nicht kommerzielle Angebote setzen Onlinewerbung ein, um zumindest einen Teil der mit der Bereitstellung verbundenen Kosten zu decken.

Onlinewerbung kann damit die Bereitstellung bestimmter Angebote ermöglichen und einen Beitrag zur Vielfalt im Wettbewerb leisten. Auch im Onlinebereich ist es beispielsweise über Bannerwerbung möglich, Werbung ohne die Erhebung von Nutzerdaten zu schalten.

Gegenüber anderen Werbeformen bietet die zielgerichtete Onlinewerbung allerdings aufgrund der technisch angelegten individualisierten Bereitstellung von Inhalten für den Nutzer auch die Möglichkeit, auf die vermutlichen individuellen Interessen der Nutzer abgestimmte Informationen und Werbebotschaften zu liefern. Hierdurch steigt die Wahrscheinlichkeit, dass ein Werbeinhalt vom Empfänger als relevant erachtet wird. Dies erhöht wiederum die erzielbaren Gewinne je angezeigter Werbung. Damit kann sich auch die Menge der ungezielten Werbung reduzieren, die notwendig ist, um eine Finanzierung des Webangebots zu erreichen. Es besteht dabei aber keine Garantie, dass tatsächlich weniger Werbung eingesetzt wird.

---

[252] Vgl. nur BVerfG, Beschluss vom 26. Juni 1990 – 1 BvR 776/84, BVerfGE 82, 236, 269 – Schubart; BVerfG, Beschluss vom 24. März 1998 – 1 BvR 131/96 , BVerfGE 97, 391, 403 – Missbrauchsbezichtigung; BVerfG, Beschluss vom 10. November 1998 – 1 BvR 1531/96, BVerfGE 99, 185, 194 – Scientology; BVerfGE, 101, 361, 380 – Caroline von Monaco II.

[253] Vgl. BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich.de.

[254] Die Fraktion BÜNDNIS 90/DIE GRÜNEN hat gegen diese Textfassung des Kapitels 2.3.1.1 *Datenschutz in der Kommunikationsgesellschaft: Zum Spannungsverhältnis und Gebot der Abwägung zwischen Persönlichkeitsrechten und Kommunikationsgrundrechten* gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.3.1). Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg schließen sich diesem Sondervotum an.

Es gibt eine Vielzahl von Technologien und Vorgehensweisen (Algorithmen), mit deren Hilfe bei verhaltensbezogener Werbung (Behavioral Advertising) eine Vorhersage über das vermutliche Interesse des Werbeadressaten getroffen wird. Die Methoden nutzen in sehr verschiedener Weise und in sehr unterschiedlichem Umfang und Intensität Daten aus der aktuellen beziehungsweise vorangegangenen Internetnutzung des Werbeempfängers.

Allerdings muss verhaltensbezogene Werbung nicht unbedingt darauf beruhen, dass Informationen über das Surfverhalten der Nutzerin oder des Nutzers dauerhaft gespeichert werden. Sie kann auch über eine anonymisierte Zuordnung zu Interessenkategorien realisiert werden, die auf einer bestimmten Art der Verwendung der Cookie-Technik basiert. Diese Cookies kann der Nutzer gegebenenfalls manuell wieder entfernen. Allerdings gibt es keine Möglichkeit auszuschließen, dass Webseiten, die Cookies auf dem Rechner des Nutzers ablegen, bei diesem Nutzer auch Daten erheben.

In allen Fällen, in denen nutzungsbezogene Daten verarbeitet werden, muss es allerdings eine zentrale Voraussetzung sein, dass die Nutzer Informationen über die vorgenommene Verwendung erhalten und ihnen eine Wahlmöglichkeit zusteht, mit der sie den Einsatz solcher individualisierender Werbetechniken beeinflussen können.

Neben dem schlichten Schalten von Werbeeinblendungen werden Kunden zum Zweck der Verkaufsförderung auch gezielt angesprochen. Dies geschieht unter anderem über Anzeigen mit besonderen Angeboten oder Gutscheinen für Neukunden und Aktionen wie Treue-Boni oder Rabatten zur langfristigen Bindung von Bestandskunden.

Die eingesetzten Techniken ermöglichen es, sowohl Werbung, Zielseiten, aber auch Angebote und Preise in Echtzeit auf die speziellen Verhaltensweisen einer Nutzerin oder eines Nutzers auszurichten. Durch die Techniken des so genannten Targeting ist es teilweise möglich, den Nutzer beim Besuch der Seite wiederzuerkennen, das jeweilige Verhalten zu erfassen und Webinhalte und -services dementsprechend dynamisch den Nutzerpräferenzen anzupassen. Für die Nutzer der Seite ist es dabei nicht mehr erkennbar, ob es sich um für sie bereits angepasste Webseiten und Werbeangebote oder aber Standardwebseiten handelt, die für alle Nutzer gleich sind.[255] Oftmals werden darüberhinaus auch Kombinationen mehrerer Techniken eingesetzt.

Jenseits des Schutzes der Privatsphäre sind daher die Auswirkungen auf die Marktposition der Nutzer beziehungsweise Verbraucher im Internet erheblich und müssen in Transparenz- sowie Einwilligungserfordernissen berücksichtigt werden.

Die Zulässigkeit, Transparenz- und Einwilligungserfordernisse hängen wesentlich von den eingesetzten Techniken, der Sensibilität der erhobenen Daten und der Datennutzung ab. So ist von Bedeutung, ob Nutzungsdaten aggregiert erhoben sowie verarbeitet werden und eine individualisierte Auswertung nicht beabsichtigt ist. Relevant ist dabei auch, ob sie pseudonymisiert oder anonymisiert werden.

Ebenso ist relevant, ob die Datenverarbeitung durch den Anbieter der Webseite selbst erfolgt oder ob die Daten durch Dritte erhoben und verwendet werden, die an dem Leistungsverhältnis gar nicht beteiligt sind. Während die Datenverarbeitung im ersten Fall auf Basis der vom Webseitenanbieter bereitgestellten Datenschutzerklärung transparent gemacht werden kann und die Nutzer die Möglichkeit erhalten, gegenüber einem klar identifizierbaren Ansprechpartner von ihrem Wahlrecht hinsichtlich der Datenerhebung und -verwendung Gebrauch zu machen, ist im letzteren Fall die geforderte Transparenz für die Nutzer oft nicht mehr gegeben und es ist ihnen häufig nicht möglich, Einfluss auf die Datenerhebung und -verwendung zu nehmen.

Die Kontrolle der Nutzer wird auch davon beeinflusst, ob die Daten – etwa in Form von Cookies – auf ihrem Gerät und damit in ihrem Herrschaftsbereich gespeichert werden, sodass sie beispielsweise über Browser-Einstellungen Einfluss darauf nehmen können, oder ob gesammelte Daten zentral und damit ihrem Zugriff entzogen gespeichert werden.

Schließlich können besondere Umstände einen besonders schwerwiegenden Eingriff darstellen und deshalb auch unzulässig sein. Dies ist etwa der Fall, wenn für die zielgerichtete Ansprache (Targeting) auch sensible Daten verwendet werden, wie etwa Informationen über Gesundheit oder sexuelle Orientierung. Problematisch ist auch, wenn Daten aus besonders geschützten Bereichen, wie etwa der Individualkommunikation, gewonnen werden, etwa durch die Analyse von E-Mail-Inhalten. Besondere Fragen wirft auch die übergreifende Nachverfolgung (Tracking) des Surfverhaltens einzelner Nutzer über eine Vielzahl von Webangeboten hinweg auf, da hier nicht nur Informationen bezüglich der Nutzung eines bestimmten Angebots, sondern ein umfassendes Bewegungsprofil der Nutzer im Netz gewonnen werden.

2.3.1.3 Bildung von Persönlichkeitsprofilen/ Tracking über die Grenzen einzelner Webseiten hinweg

Personenbezogene Daten können in unterschiedlicher Intensität Aussagen über Personen und deren soziale Beziehungen enthalten. Je nach Umfang und Qualität der Daten lassen sich diese durch Zusammenführung aus unterschiedlichen sozialen Zusammenhängen zu Persönlichkeitsbildern verdichten. Übertragen auf das Internet entspricht dem etwa die Zusammenführung von Daten über das Nutzungsverhalten von unterschiedlichen Webange-

[255] Zu den Geschäftsmodellen in der Onlinewerbung, eine Übersicht über die eingesetzten Techniken, deren Erkennbarkeit und Beeinflussbarkeit durch die Verbraucher und dem Einsatz von Profilbildung im Besonderen siehe Klein, A./Leithold, Franziska/Zell, Christine/Roosen, Jutta: Digitale Profilbildung und Gefahren für die Verbraucher. TU München, Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes e. V., November 2010. Zusammenfassung online abrufbar unter: http://www.vzbv.de/mediapics/digitale_profilbildung_tu_muenchen_leithold_2010.pdf

boten. Entsprechende Geschäftsmodelle reichen von der Zusammenführung von Nutzungsdaten innerhalb des Webangebotes eines einzelnen Anbieters bis hin zu komplexen webseitenübergreifenden Kooperationen unterschiedlicher Anbieter, oftmals unter Einschaltung von Dienstleistern (zum Beispiel DoubleClick, „Gefällt-mir“-Button). Aufgegriffen wurde der Begriff der Profilbildung unter anderem vom Bundesverfassungsgericht im Volkszählungsurteil.[256] Das Gericht betont das Verbot von Profilbildungen, die geeignet sind, die Persönlichkeit von Menschen vollständig oder nur teilweise abzubilden. Befürchtet wird, dass die in öffentlicher Hand und zu ganz unterschiedlichen Zwecken gesammelten Datenbestände zusammengeführt werden und ein nahezu lückenloses Bild der Bürger zum Zweck der Herrschaftsausübung schaffen könnten. Als Risiko im Kontext der Privatwirtschaft gilt der Missbrauch entsprechend reichhaltiger Profile und die oftmals intransparent bleibende Beeinflussung der wirtschaftlichen Entscheidungen der Verbraucher durch gezielte Werbung. Infolge der technischen Entwicklung spielen Fragen der Profilbildung nicht nur im öffentlichen Bereich (zum Beispiel Rasterfahndungen), sondern auch im nicht-öffentlichen Bereich eine große Rolle. Dabei ist zwischen ganz unterschiedlichen Arten von Profilen und deren Nutzung zu unterscheiden.

Im Internet sind für bestimmte Nutzergruppen angepasste oder sogar besonders detaillierte und personalisierte Angebote möglich und gängig. Seit Jahren werden Auswertungstools verwendet, mit denen das Nutzerverhalten auf einer Webseite statistisch erfasst und analysiert werden kann. Die dabei untersuchten Daten werden häufig nur aggregiert und/oder pseudonymisiert ausgewertet. Ob es sich dabei um anonyme und damit nicht mehr dem Anwendungsbereich der Datenschutzgesetze unterfallende Profildaten handelt, ist jedoch umstritten. In einigen Fällen wird allerdings durch die Einbeziehung von personenbezogenen Webangeboten (soziale Netzwerke, Mailangebote) insgesamt eine Personenbeziehbarkeit des Profils herbeigeführt. Es besteht Einigkeit, dass solche Nutzungsprofile bei Einhaltung bestimmter Vorgaben zulässig sind.[257] Anhand dieser Nutzungsprofile können Webseiten zum Beispiel nutzerfreundlicher gestaltet werden. Durch eine entsprechende Optimierung der Webseite können Effizienzgewinne bei der Bewerbung und dem Verkauf von Produkten erreicht werden.

Auch andere Methoden der Profilbildung wie etwa das so genannte Scoring, das heißt die Bewertung von Personen anhand der Zuordnung von statistischen Erfahrungswerten, sind in der Wirtschaft üblich. Der Gesetzgeber hat darauf reagiert und Grenzen wie das Verbot automatisierter Einzelbewertung sowie zusätzliche Transparenzanforderungen geschaffen. Die Ergebnisse der Profilbildung beim Scoring basieren zumeist auf statistischen Annahmen, die ohne Weiteres auf Individuen angewandt werden. Entscheidungen zu Personen, die auf Grundlage solcher Profile getroffen werden, basieren damit nicht mehr auf individuellen Gegebenheiten, obwohl es im Einzelfall stets ganz anders sein kann als im statistischen Mittel. Dementsprechend können Diskriminierungen bis hin zur Ausgrenzung ganzer Gruppen die Folge sein. Diese Nichtberücksichtigung individueller Verhältnisse berührt Grundrechte des Persönlichkeitsschutzes wie auch die Menschenwürde.

Weitergehende Analysen zum Beispiel auf der Grundlage aller zu einer Person verfügbaren Informationen (etwa webseitenübergreifend wie durch den „Gefällt-mir“-Button von Facebook) sind denkbar. Durch die Möglichkeit allgegenwärtiger Datenverarbeitung (Ubiquitous Computing) und Vernetzung potenzieren sich sowohl die Möglichkeiten als auch das Risikopotenzial von Profilbildung im Internet. Dementsprechend wird auch und gerade im Kontext des Internets die eingehende Regulierung des zulässigen Einsatzes der Profilbildung gefordert (so zuletzt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrem Eckpunktepapier zur Modernisierung des Datenschutzes).[258] Diskutiert werden in diesem Zusammenhang eine gesetzliche Definition der Profilbildung und die Schaffung von gesetzlichen Grundlagen, die dem besonderen Gefährdungspotenzial von Profilbildungen Rechnung tragen. Für die Beurteilung des Gefährdungspotenzials kommt es maßgeblich darauf an, welche Art von Daten in welcher Form, zu welchem Zweck und in welchem Umfang erfasst sowie ausgewertet werden können. Gefordert wird auch eine Anonymisierung, soweit dies möglich ist. Zusätzliche Transparenzanforderungen wie die Pflicht zur Erläuterung von Profilbildungsverfahren sollen Verbrauchern helfen, die Folgen der Nutzung von entsprechenden Angeboten einschätzen zu können.

2.3.2 Ausgestaltung und Reichweite von Transparenzinstrumenten (Informationspflichten, Auskunftsrechte)

Transparenz und damit Informationen sind Kernelemente für informierte Entscheidungen und Aktivitäten der Aufsichtsbehörden, von Wettbewerbern beziehungsweise anderen Unternehmen und Verbraucherinnen und Verbrauchern. Eine wesentliche Voraussetzung für die auch praktische Durchsetzung des Datenschutzes – und damit der Realisierung des Rechts auf informationelle Selbstbestimmung – ist die Kenntnis über das Recht beziehungsweise die eigenen Rechte einerseits wie auch über die tatsächlich durchgeführte Datenerhebung und -verarbeitung andererseits.

[256] Vgl. BVerfGE 65, 1 – Volkszählung.

[257] Vgl. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 26./27. November 2009: Datenschutzkonforme Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile

[258] Vgl. Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile

Transparenz für die Nutzer setzt voraus, dass sich der Nutzer seinem Bedarf entsprechend und frühzeitig über Art und Umfang der Datenerfassung und -verarbeitung informieren kann. Dabei ist es angesichts oft komplexer technischer Zusammenhänge besonders wichtig, für die Verständlichkeit der vermittelten Informationen zu sorgen.

Wie wichtig Transparenz für die Nutzer ist, zeigt das Beispiel der Einführung neuer Technologien und Dienste: Am Anfang steht, wie zum Beispiel bei Apps, das positive Nutzungserlebnis und die Freude über den Mehrwert der Innovation. Ohne vorherige Information kämen erst nach und nach Erfahrungen dazu, die aufhorchen und die Frage nach dem Datenschutz und möglichen Missbrauchsszenarien laut werden lassen. Die berechtigte Sorge wird dabei aus dem Umstand genährt, dass Dinge im Hintergrund passieren, die unbekannt und vermeintlich nicht beeinfluss- beziehungsweise kontrollierbar sind.

Hier ist der Ansatz für Transparenz und deren Instrumente. Die Nutzerinnen und Nutzer sollen in die Lage versetzt werden zu verstehen, was mit den Daten passiert, und zu entscheiden, ob sie das so und in diesem Umfang wollen.

Letztlich muss der Nutzer derjenige bleiben, der diese Entscheidung trifft. Damit wird die Frage der Reichweite beziehungsweise der Grenze von Transparenzinstrumenten angesprochen.

Ziel sollte also die verständliche, neutrale Information über die tatsächlichen technischen Vorgänge sein. Dem Nutzer muss klar werden, wer persönliche Daten verarbeitet, wie, in welchem Umfang sowie zu welchen Zwecken dies geschieht und wer sein Ansprechpartner für Fragen sowie – besonders wichtig – die Ausübung seiner Selbstbestimmung über die Datenverarbeitung ist.

Das Bundesdatenschutzgesetz, das Telemediengesetz und das Telekommunikationsgesetz sehen jeweils bereits eine Reihe von Transparenzinstrumenten vor. Diese Regelungen sind somit eine gesetzliche Konkretisierung des Rechts auf informationelle Selbstbestimmung.

Informationspflichten von Diensteanbietern

Diensteanbieter haben grundsätzlich die Pflicht, die Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten zu unterrichten (§ 13 TMG, § 33 BDSG). Die Informationspflichten sollen sicherstellen, dass die Adressaten Kenntnis von der Datenverarbeitung erhalten. Es muss über die Identität der verantwortlichen Stelle informiert werden, damit bekannt ist, wer die Daten erhebt und als Adressat eines Auskunftsanspruchs zur Verfügung steht. Über sämtliche Zweckbestimmungen der Verarbeitung und Nutzung der Daten muss informiert werden, soweit sie über die zur Vertragsdurchführung erforderlichen Daten hinausgehen. Der oder die Empfänger der Daten müssen zumindest als Kategorie bekannt sein (vergleiche § 33 Absatz 1 Satz 3 BDSG). Eine namentliche Nennung der Empfänger ist jedoch nicht erforderlich, sodass eine lückenlose Verfolgung des Weges der Daten nicht ohne weitere Informationen beziehungsweise Auskunftsersuchen möglich ist. Dieses Wissen ist für eine Person jedoch notwendig, um die Auskunftsrechte bei allen Stellen, die Daten über sie haben, geltend machen zu können.

Die Unterrichtung muss in einer allgemein verständlichen Form geschehen. Damit soll gewährleistet werden, dass die Bürgerinnen und Bürger eine informierte Entscheidung zur Preisgabe ihrer persönlichen Daten treffen und gegebenenfalls eine Einwilligung verweigern können. In der Regel sind diese Informationen in den allgemeinen Geschäftsbedingungen (AGB) und Nutzungsbedingungen der Diensteanbieter enthalten. Da es sich zumeist um umfangreiche und aufgrund gesetzlicher Vorgaben rechtssicher zu formulierende Texte handelt, sind sie für viele Menschen oftmals nicht in Gänze nachvollziehbar und nur schwer zu verstehen.

Auskunftsrechte des Betroffenen

Neben der Informationspflicht der Diensteanbieter bei Erhebung, Speicherung und Verwendung von personenbezogenen Daten sind in § 34 BDSG umfassende Auskunftsrechte der Betroffenen festgeschrieben. Darin werden diese berechtigt, jederzeit und bedingungsfrei zu erfahren, welche personenbezogenen Daten von einer verantwortlichen Stelle über sie erhoben, verarbeitet oder genutzt werden, woher die Daten stammen, an wen die Daten weitergeleitet und zu welchem Zweck sie gespeichert werden. Unter bestimmten Bedingungen kann die verantwortliche Stelle die Auskunft allerdings verweigern, etwa zur Wahrung von Geschäftsgeheimnissen (vergleiche § 34 BDSG). Wenngleich diese Auskunftsrechte für Betroffene ein starkes Instrument zur Wahrung der informationellen Selbstbestimmung sind, erscheint die praktische Nutzung in einer Umgebung, in der immer mehr Anwendungen im Alltag personenbezogene Daten nutzen, zunehmend weniger handhabbar.

In letzter Zeit ist deshalb die Idee des so genannten Datenbriefs im Gespräch. Unternehmen, Behörden oder sonstige Institutionen könnten gesetzlich verpflichtet werden, Bürgerinnen und Bürger regelmäßig darüber zu informieren und ihnen zu erläutern, welche Daten zu welchem Zweck über sie gespeichert werden. Dies käme einem Paradigmenwechsel gleich: Das derzeitige Auskunftsrecht würde durch eine Informationspflicht ergänzt. Der Betroffene müsste also nicht mehr selbst aktiv werden, um zu erfahren, welche Daten wo über ihn gespeichert sind, sondern würde automatisch darüber benachrichtigt.

Für den Datenbrief wird angeführt, dass viele Betroffene derzeit oft gar nicht wüssten, wo überall Daten über sie gespeichert werden. Sie könnten daher gar nicht von ihrem gesetzlich eingeräumten Auskunftsrecht Gebrauch machen. Dieser Anspruch laufe daher häufig ins Leere. Mit dem Datenbrief würde zudem das Verantwortungsbewusstsein der für die Datenverarbeitung verantwortlichen Stellen gestärkt. Sie würden unter Umständen genauer prüfen, ob und wie lange personenbezogene Daten tatsächlich gespeichert werden müssten.

Gegen den Datenbrief wird angeführt, dass er zunächst bei vielen datenverarbeitenden Stellen zu einer zentralen Zusammenführung der Daten führen könnte. An diese Konzentration von Daten müssten dann nicht nur höhere Sicherheitsanforderungen gestellt werden, sondern dies könnte auch wegen einer damit verbundenen Möglichkeit der verstärkten Profilbildung zu einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung führen. Auch die praktische Umsetzung des Datenbriefs wird als zu bürokratisch und kostenintensiv für die betroffenen Unternehmen kritisiert.

Informationspflichten bei „Datenpannen“

Die „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten“ (§ 42a BDSG) verpflichtet verantwortliche Stellen im nicht-öffentlichen Bereich, die Betroffenen sowie die zuständigen Aufsichtsbehörden umgehend zu informieren, wenn gespeicherte sensible personenbezogene Daten unrechtmäßig an Dritte gelangen. Diese Regelung wurde jedoch erst im Jahr 2009 in das BDSG aufgenommen. Ursache hierfür waren vorhergegangene unerlaubte und missbräuchliche Erhebungen und Verarbeitungen von personenbezogenen Daten in der Wirtschaft.

Ziel aller Informationspflichten ist es, Transparenz über die Speicherung und Verarbeitung von Daten herzustellen. Diese Transparenz ist Voraussetzung dafür, die informationelle Selbstbestimmung tatsächlich ausüben zu können. Ohne ausreichende Transparenz kann keine informierte Einwilligung erteilt werden. Wenn Betroffene in die Lage versetzt werden sollen, bereits nach dem Bundesdatenschutzgesetz bestehende Auskunfts-, Lösch-, Widerspruchs- und Berichtigungsrechte auch tatsächlich geltend machen zu können, ist die Kenntnis notwendig, wer welche Daten zu welchem Zweck gespeichert hat.

2.3.3 Cloud-Computing

Beschreibung

Angesichts stetig steigender Datenvolumina und einer wachsenden mobilen Nutzung von Daten stellt sich dem Nutzer – sei es Privatperson oder Unternehmer – vermehrt die Frage „Wohin mit den Daten, die anfallen?“ und „Wie kann ich Datenverarbeitungsprozesse effizienter und kostengünstiger gestalten?“. Als Lösung wird zunehmend das so genannte Cloud-Computing angeführt, übersetzt „Datenverarbeitung in der Wolke“.

Von Cloud-Computing wird gesprochen, wenn eine oder mehrere IT-Dienstleistungen, wie Infrastruktur (Rechenleistung, Hintergrundspeicher etc.), Plattform oder Anwendungssoftware aufeinander abgestimmt und nach tatsächlicher Nutzung abrechenbar über ein Netz durch Dritte bereitgestellt werden.[259] Obwohl die Onlinespeicherung von Daten, Online-Adressbücher, Online-Kalender oder etwa die webbasierte Nutzung von E-Mail-Diensten bereits als alltägliche Cloud-Anwendungen von vielen genutzt werden, kann zum gegenwärtigen Zeitpunkt noch nicht davon ausgegangen werden, dass der Begriff und die dahinter liegende Technik des Cloud-Computings geläufig sind. Es ist davon auszugehen, dass sich Cloud-Computing in den nächsten Jahren vor allem im Bereich der Geschäftsanwendungen und der Serverkapazitäten immer weiter etablieren wird.

Angebotene Dienstleistungen im Cloud-Computing können unter anderem bereitgestellter Speicher oder Rechenzeit sein, aber auch komplette Datenverarbeitungsverfahren. Beim Cloud-Computing wird zum einen nach der Art der in der Cloud angebotenen Dienstleistung unterschieden; und zwar zwischen Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS). Zum anderen wird nach der Beschaffenheit der Cloud zwischen Private und Public Clouds unterschieden. Private Clouds sind vernetzte Rechner, die alle unter der rechtlichen Verantwortung einer einzigen datenverarbeitenden Stelle stehen.[260] Als Private Clouds werden aber auch Rechnernetze von rechtlich zueinander in einem engen Verhältnis stehenden Stellen bezeichnet, zum Beispiel Stellen der öffentlichen Verwaltung oder eines Konzerns.[261]

Eine Public Cloud ist eine öffentliche Cloud, welche von einer Vielzahl von Personen und Firmen genutzt werden kann. Die Public Cloud ist nicht auf eine bestimmte Institution, ein bestimmtes Unternehmen oder einen bestimmten Personen- oder Nutzerkreis beschränkt. Wesentliches Merkmal ist, dass sie jedermann zugänglich ist und dass der Anwender nicht mitbestimmen kann, mit welchen Anwendern er sich die Nutzung einer Hardware teilt, also mit welchen anderen virtuellen Maschinen seine virtuelle Maschine auf derselben physischen Hardware läuft.[262] Dabei wird die Rechenleistung von „Dritten“ im Sinne des Datenschutzrechts (§ 3 Absatz 8 Satz 2 BDSG) angeboten.[263] Zu den Anbietern solcher Public Clouds gehören IT-Unternehmen, wie zum Beispiel Google, Amazon, IBM, SAP oder die Deutsche Telekom. Neben diesen beiden Formen existiert auch eine Mischform von Public und Private Cloud, die Hybrid Cloud, bei der eine Nutzung von eigenen und fremden Ressourcen stattfindet.

Eine der Besonderheiten des Cloud-Computings liegt je nach Angebot in der zumeist flexiblen und grenzüberschreitenden Bereitstellung von Cloud Ressourcen durch eine Vielzahl von Beteiligten.

Offene Fragen im Bereich des Datenschutzes und der Datensicherheit beim Cloud-Computing

Die Auslagerung von Daten und Datenverarbeitung in die Cloud wirft datenschutz- und datensicherheitsrelevante

[259] Vgl. Bundesamt für Sicherheit in der Informationstechnik. Essoh, Alexander Didier: Cloud Computing und Sicherheit – Geht denn das?, Folie 4. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/4GS_Tag/07_essoh_bsi.pdf?__blob=publicationFile

[260] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (679).

[261] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

[262] Vgl. Birk, Dominik/Wegener, Christoph: Über den Wolken: Cloud Computing im Überblick. DuD 2010, 641 (642).

[263] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

Fragestellungen auf. Wenn Unternehmen ihre IT-Strukturen in eine Cloud auslagern, wird der Umfang der Datensicherheit und des Datenschutzes vom Anbieter der Cloud bestimmt.

Datensicherheit

Das zentrale Problem hinsichtlich der Datensicherheit besteht darin, die Integrität (Datenveränderungen können erkannt werden) und Vertraulichkeit (nur Befugte können auf Daten zugreifen) der Datenverarbeitung sowie die Verfügbarkeit (Daten stehen in einem angemessenen Zeitraum zur Verfügung) zu gewährleisten.[264] Wie aktuell die Datensicherheit auf Netzwerk- und Datenebene in der Cloud gewährleistet wird, welche möglichen Probleme es gibt und inwieweit sich daraus politischer Handlungsbedarf ergibt, sollte aufgrund des Sachzusammenhangs von der Projektgruppe Zugang, Struktur und Sicherheit im Netz geprüft werden.

Datenschutz

Bei manchen Formen des Cloud-Computings stellen sich besondere Herausforderungen, weil Rechtsgrundlagen wie Auftragsdatenverarbeitung oder Übermittlung das Cloud-Computing nicht vollständig erfassen. Zudem werden damit typische, bereits bekannte Probleme des Outsourcings nicht nur potenziert, sondern sie gewinnen auch eine neue Qualität. Im Hinblick auf Rechenprozesse kann nicht mehr mit Bestimmtheit gesagt werden, auf welchen der oftmals weltweit verbundenen Server und damit bei welchen Beteiligten konkret welche Datenverarbeitungsprozesse vollzogen werden. Dies führt zu rechtlichen Unsicherheiten bei der Nutzung und dem Betreiben entsprechender Angebote.

Gerade im Fall eines grenzüberschreitend angelegten Cloud-Computings ergeben sich Fragen nach der Verantwortlichkeit sowie den Zugriffsmöglichkeiten Dritter. Um die Datenverarbeitung innerhalb der EU zu harmonisieren, wurde die europäische Datenschutzrichtlinie geschaffen. Da der Umstand einer grenzüberschreitenden Datenverarbeitung innerhalb des europäischen Binnenmarktes kein rechtliches Hindernis darstellen soll, dürfen gemäß Artikel 1 Absatz 2 DSRL personenbeziehbare Daten im gesamten EWR verarbeitet werden.[265] Für eine Anwendbarkeit nationalen Rechts kommt es gemäß Artikel 4 Absatz 1 Buchstabe a und b DSRL deshalb darauf an, in welchem Mitgliedstaat die datenverarbeitende Niederlassung ihren Sitz hat.[266] Damit auch Unternehmen, die keine Niederlassung im EWR haben, personenbezogene Daten verarbeiten können, wurde in § 1 Absatz 5 Satz 3 BDSG bestimmt, dass diese Unternehmen einen Datenschutzbeauftragten innerhalb der EU benennen, welcher für die Einhaltung der Richtlinien verantwortlich ist.

Hinsichtlich der Verantwortlichkeit ergibt sich aus Artikel 2 Buchstabe d DSRL, dass derjenige für die Verarbeitung verantwortlich ist, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Dies ist grundsätzlich der Cloud-Nutzer und nicht der Anbieter.

Insgesamt sind alle Datensätze, die nicht als personenbeziehbar gelten (§ 3 Absatz 1 BDSG) zur Verarbeitung in Clouds vollkommen unproblematisch. Datenschutzrelevant ist die Form der Nutzung des Cloud-Computings nach deutschem Recht nur dann, wenn personenbezogene Daten (§ 3 Absatz 1 BDSG) verarbeitet werden. Da im Rahmen der Nutzung cloud-basierter Dienstleistungen oft personenbezogene Daten auf dem System des Cloud-Anbieters gespeichert sowie verarbeitet werden und bei grenzüberschreitenden Systemen auch auf Speichermedien europa- beziehungsweise sogar weltweit verteilt sind, stellt sich die Frage nach der Behandlung dieser Verlagerung der Daten in die Cloud. Aus rechtlicher Sicht kann es sich um eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG handeln. Diese erfährt datenschutzrechtlich die Grenzen ihrer Zulässigkeit zum einen dort, wo dem Verantwortlichen (dem Nutzer der Cloud) durch den Dienstleister keine Angaben über Art und Ort der Verarbeitung und Sicherungsmaßnahmen gemacht werden. Zum anderen ist dies der Fall, wenn die datenverarbeitende Stelle in einem Staat außerhalb Deutschlands, eines anderen Mitgliedstaates der EU oder des EWR liegt, in dem kein vergleichbares Datenschutzniveau existiert. In diesem Fall handelt es sich um eine Weitergabe an „Dritte" im Sinne des § 3 Absatz 8 BDSG, wobei der Gesetzgeber unterstellt, dass bei derartigen Übermittlungskonstellationen besondere persönlichkeitsrechtliche Risiken entstehen, weil von der verantwortlichen Stelle, vom Betroffenen oder von den staatlichen Aufsichtsbehörden keine hinreichende Kontrolle der Datenverarbeitung möglich ist.[267]

Hinzu kommt, dass die in § 11 Absatz 2 BDSG geforderte „sorgfältige" Auswahl des Auftragnehmers „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen" in der Praxis nur schwer einzuhalten ist, da unter anderem der Auftragnehmer dem Auftraggeber in der Regel nicht derart tiefgehende Einblicke in seine IT-Struktur gewährt.

Je nach verwendetem Angebot (beispielsweise Verteilung der Daten auf mehrere weltweit verteilte Server) kann die Verlagerung der Daten in die Cloud zu einer Erhöhung der Gefahr von Zugriffsmöglichkeiten durch Dritte führen. Wichtig ist daher, dass der früher selbst Datenverarbeitende die Herrschaft über die Daten bewahrt und Kenntnis und Einfluss über die ergriffenen Sicherungsmaßnahmen hat.

---

[264] Vgl. Heidrich, Jörg/Wegener, Christoph: Sichere Datenwolken – Cloud Computing und Datenschutz. MMR 2009, 803 (804).

[265] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

[266] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

[267] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

Folgeproblem der Verlagerung und der Verteilung der Daten auf europa- und weltweite Server ist eine erschwerte Datenschutzkontrolle. Eine Datenschutzkontrolle durch die Aufsichtsbehörden ist auf das jeweilige Landes- beziehungsweise Bundesterritorium begrenzt. Europaweit kann gegenseitig eine Amtshilfe der Aufsichtsbehörden erfolgen. Über das europäische Territorium hinaus sind koordinierte oder gemeinsame Kontrollen in Clouds mit Drittlandsbezug praktisch nicht möglich.[268] Dies eröffnet datenschutzrechtlich verantwortlichen Stellen die Möglichkeit, sich Datenschutzkontrollen zu entziehen, in dem gezielt Clouds mit Drittlandsbezug genutzt werden. Daneben ist besonders problematisch, wenn die Datenverarbeitung in Staaten erfolgt, die nicht nur keinen ausreichenden Datenschutz gewährleisten, sondern auch bewusst und gezielt gegen Menschenrechte verstoßen und den Zugriff auf Daten in der Cloud zu politischer Überwachung und Verfolgung nutzen.[269]

Der Ort, wo die Daten gespeichert und verarbeitet werden, spielt also eine zentrale Rolle. Dies zeigt sich auch für Daten, welche für Steuerzwecke benötigt werden. Diese dürfen gemäß § 146 Absatz 2 Satz 1 Abgabenordnung (AO) nur im Inland gespeichert werden. Auch hier stellt sich das Problem bei länderübergreifenden Netzen und der Information, in welchem Land die Daten gelagert und verarbeitet werden. Nach § 146 Absatz 2a AO kann die zuständige Finanzbehörde bewilligen, dass die Finanzdokumente auch außerhalb der EU oder des EWR archiviert werden.[270] Auch hier könnten die Steuerermittlungsbehörden vor Probleme gestellt werden, weil nicht ohne Weiteres ein Zugriff auf die Daten erfolgen kann.

Im Ergebnis ist festzuhalten, dass es noch offene datenschutzrechtliche Fragen gibt, wenn personenbezogene Daten in die Cloud verlagert werden. Dies kann die Nutzung, aber auch die sich bietenden Möglichkeiten und Innovationen des Cloud-Computings einschränken. Bisher können datenschutzrechtliche Erfordernisse nur durch besonders umfangreiche und detaillierte Vertragsvereinbarungen gewährleistet werden. Für die Ermittlung von Straftaten und Ordnungswidrigkeiten stellt die Speicherung von Daten in der Cloud dann ein Problem dar, wenn durch die Art und den Ort der Datenverarbeitung ein Zugriff für die Ermittlungsbehörden nicht möglich ist.[271] Im Inland stehen Staatsanwaltschaften und auf Anordnung auch ihren Ermittlungspersonen gemäß § 110 Absatz 3 StPO seit dem Jahr 2008 entsprechende Befugnisse auf Durchsicht von Speichermedien zu.

2.3.4 „Verfallsdaten“ im Internet, regelmäßig erneuerbare Zustimmungspflicht

Im Kontext des Internets bereitet die Rückgängigmachung einer einmal gewollten Datennutzung oder auch Datenveröffentlichung bei geänderter Einschätzung besondere Schwierigkeiten.

Schwierig stellt sich die Lage bei veröffentlichten Daten dar. Aufgrund der einfachen Vervielfältigung digitaler Daten im Internet und wegen der technischen Gegebenheiten ist davon auszugehen, dass einmal veröffentlichte Daten nicht mehr „zurückzuholen“ sind. Selbst wenn es gelingt, die weitere Verwendung oder Veröffentlichung an einer bestimmten Stelle zu unterbinden, ist bei Daten anzunehmen, dass sie an anderer Stelle bereits dupliziert wurden.

Seit einigen Jahren wird mit zunehmender Bedeutung des Internets auch die Diskussion über ein „Recht auf Vergessen“ geführt. Allerdings sind die hierfür in der Diskussion verwendeten Begrifflichkeiten noch sehr unterschiedlich. So wird neben dem „Recht auf Vergessen“[272], beispielsweise auch vom „programmierten Vergessen“[273], „Verfallsdaten“ oder dem „digitalen Radiergummi“[274] gesprochen. Die unterschiedlich verwendeten Terminologien haben teilweise nicht nur unterschiedliche Argumentationsansätze, sondern auch eine sehr unterschiedliche Reichweite. Auch wenn sie daher nicht vollständig als Synonym für das „Recht auf Vergessen“ verwendet werden sollten, haben sie einen gemeinsamen Kerngedanken. Demnach sollen die Nutzer des Internets mit Hilfe einer oder mehrerer technischer Lösungen selbst darüber bestimmen können, wie lange ihre personenbezogenen Daten im Internet gespeichert bleiben sollen beziehungsweise nach welcher Zeit der „menschliche Vorgang“ des Vergessens beginnen soll. Sie können im Idealfall bereits mit dem Einstellen der personenbezogenen Daten festlegen, dass eine (vollständige) Löschung der Daten an einem zuvor bestimmten Datum in der Zukunft erfolgen soll. Aufgrund der nahezu unbegrenzten Speicher- und Vervielfältigungsmöglichkeiten des Internets stellt dies die bisherigen technischen Gegebenheiten vor besondere Anforderungen.

Bereits jetzt existieren einzelne webbasierte Anwendungen, die es der Nutzerin und dem Nutzer ermöglichen sollen, die Abrufbarkeit der Daten zeitlich zu begrenzen. Allerdings fehlt es bisher an einer Gesamtlösung für alle Bereiche des Internets und insbesondere für die besonders datenintensiven sozialen Netzwerke. Erste technische Ansätze hierfür wurden bereits vor zwei Jahren in den USA entwickelt. Die University of Washington programmierte eine entsprechende Technik für den Verfall der eigenen personenbezogenen Daten, die auch auf soziale

[268] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (684).
[269] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (684).
[270] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).
[271] Vgl. Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).
[272] Mayer-Schönberger, Viktor: Delete: The Virtue of Forgetting in the Digital Age. 2009. Rosen, Jeffrey: The Web means the End of Forgetting. The New York Times vom 21. Juli 2010. Online abrufbar unter: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html
[273] Bull, Hans Peter: Persönlichkeitsschutz im Internet. NVwZ 2011, 257 (260).
[274] Vgl. dazu die Rede des damaligen Bundesinnenministers Dr. Thomas de Maizière zu den Grundlagen für eine gemeinsame Netzpolitik der Zukunft. Berlin, 22. Juni 2010. Thesenpapier online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/thesen_netzpolitik.pdf?__blob=publicationFile

Netzwerke angewendet werden kann.[275] Die Universität des Saarlandes stellte im vergangenen Jahr ein vergleichbares Produkt vor.[276] Beide Techniken stehen jedoch noch am Anfang der Entwicklung und verhindern keineswegs die Möglichkeit der Vervielfältigung von eingestellten personenbezogenen Daten (insbesondere Bildern). Ein „Recht auf Vergessen" kann somit aus technischer Sicht zum jetzigen Zeitpunkt nicht durchgesetzt oder gewährleistet werden.[277]

Ungeachtet dessen hat die politische und rechtliche Diskussion um ein „Recht auf Vergessen" in den letzten Monaten weiter an Fahrt gewonnen. Auch die EU-Kommission hat das „Recht auf Vergessen" als prüfungswerten Punkt für eine Überarbeitung der Datenschutzrichtlinie mit in die bevorstehende Konsultation aufgenommen.[278]

2.3.5 Privacy by Design und Privacy by Default

Privacy by Design beschreibt den Ansatz, bereits bei der Konzeption und Ausgestaltung von Technologien den Datenschutz einzubeziehen.[279] So können eventuelle nachträgliche Schwierigkeiten bei der Einhaltung datenschutzrechtlicher Vorgaben bereits im Vorfeld vermieden und verhindert werden. Eine entsprechende Korrektur im Nachhinein ist oft nur sehr mühsam und mit viel Aufwand umzusetzen.

In einer Zeit, in der zunehmend auch technische Geräte des Alltags beginnen, personenbezogene Daten zu erfassen und über das Internet zu kommunizieren, werden die Herausforderungen an die Sicherung des Rechts auf informationelle Selbstbestimmung und den Vollzug des geltenden Datenschutzrechts wachsen.

Die konsequente und frühzeitige Umsetzung von Privacy by Design stellt auch eine Möglichkeit zur Problemlösung im Bereich der Einwilligung nach § 4 BDSG dar. Elemente von Privacy by Design können beispielsweise eine grundsätzliche Verschlüsselung von Daten, die Löschung von Daten nach Funktionserfüllung oder technische Vorkehrungen zur Einhaltung des Zweckbindungsgrundsatzes sein.[280] Sie unterstützen damit Nutzerinnen und Nutzer technischer Geräte und helfen ihnen, ihr gesetzlich gewährleistetes Recht auf informationelle Selbstbestimmung auch tatsächlich ausüben zu können. Gleichzeitig konkretisieren sie auf diese Weise das Gebot der Datensparsamkeit und -vermeidung.

In Ergänzung zu Privacy by Design stellt das Prinzip des Privacy by Default eine wichtige Option zur Gestaltung von elektronischen Diensten und Anwendungen wie etwa sozialen Netzwerken oder so genannten Location-based Services (standortbezogene Dienste) dar. Nach diesem Prinzip gestaltete Dienste sehen ab dem ersten Moment der Nutzung die jeweils höchstmöglichen nutzbaren Datenschutzeinstellungen vor. Nutzerinnen und Nutzer können dann mittels eines so genannten Opt-out die Einstellungen des Datenschutzniveaus nach ihren Vorstellungen anpassen. Eine konsequente Anwendung des Prinzips Privacy by Default erscheint gerade angesichts der Vielfalt der einzelnen technischen Einstellungen vieler webbasierter Angebote und der oftmals nicht leicht erkennbaren Konsequenzen sinnvoll.

Privacy by Design und Privacy by Default orientieren sich an den Vorgaben der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) und damit an einer zentralen Leitlinie des Datenschutzrechts. Sie sind als immanente Grundprinzipien geeignet, den gegenwärtigen und zukünftigen Herausforderungen für einen Datenschutz wirksam und effektiv zu begegnen.

2.3.6 Datenweitergabe und -handel

Personenbezogene Daten (wie beispielsweise Adress- und Kontaktdaten oder auch Daten zum Einkaufsverhalten) sind Gegenstand von Transaktionen. Sie werden zwischen Unternehmen verkauft, vermietet oder aber getauscht.

Neben legalem Handel mit Daten kommt es im und über das Internet zu einem illegalen Handel mit personenbezogenen Daten (national wie international). Dieser illegale Handel umfasst sowohl Daten, die unter bestimmten Voraussetzungen gehandelt werden dürften (zum Beispiel Adressdaten oder Daten zum Einkaufsverhalten), als auch Daten, deren Handel in jedem Fall unzulässig ist (zum Beispiel Passwörter zu E-Mail-Konten).

Darüber hinaus wurde in der Vergangenheit aber auch eine Grauzone im Bereich der Datenweitergabe und des Datenhandels festgestellt.[281] Diese Grauzone erstreckte sich insbesondere auf die Bereiche des E-Mail- und Telefon-Marketings, die beide nicht unmittelbar unter das Bundesdatenschutzgesetz fallen, sondern vornehmlich dem Telemediengesetz (vergleiche § 6 TMG), dem Telekommunikationsgesetz (vergleiche § 95 TKG) und dem Gesetz gegen den unlauteren Wettbewerb (vergleiche § 7 Absatz 2 Nummer 2, 3 UWG) unterliegen. Aber auch bei

[275] Vgl. Hickey, Hannah: This article will self-destruct: A tool to make online personal data vanish. Online abrufbar unter: http://www.washington.edu/news/archive/id/50973

[276] Vgl. Universität des Saarlandes: X-pire! – Wie man dem Internet das „Vergessen" beibringt. Online abrufbar unter: http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/

[277] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben ein ergänzendes Sondervotum zu diesem Absatz abgegeben (siehe Kapitel 4.1.3.2).

[278] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Gesamtkonzept für den Datenschutz in der Europäischen Union" vom 4. November 2010, S. 8, KOM (2010) 609.

[279] Vgl. Schaar, Peter: Privacy by Design. Identity in the Information Society. 2010, 267-274.

[280] Vgl. Unterrichtung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung. Technikfolgenabschätzung (TA) / Zukunftsreport – Ubiquitäres Computing vom 6. Januar 2010, Bundestagsdrucksache 17/405, S. 126.

[281] Vgl. S. 5 des Neunzehnten Datenschutz- und Informationsfreiheitsberichts der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen für die Jahre 2007 und 2008, 2009. Online abrufbar unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/19_DIB/DIB_2009.pdf

anderen Angeboten, die dem Bundesdatenschutzgesetz unmittelbar unterliegen, fällt eine Abgrenzung zwischen zulässiger Handlung und möglichem Verstoß gegen datenschutzrechtliche Vorschriften nicht immer leicht. Dies gilt insbesondere für die Fälle, in denen das Geschäftsmodell unter anderem darauf abzielt, personenbezogene Daten von möglichst vielen Nutzern zu erheben und gegebenenfalls an Dritte weiterzugeben. Aber auch die in der Praxis beliebte Form der Freundschaftswerbung wirft immer wieder schwierige datenschutzrechtliche Fragen auf.

Der Bereich der Datenweitergabe und des Datenhandels im Bundesdatenschutzgesetz wurde im Jahr 2009 umfangreich novelliert. Seitdem schreibt das Gesetz vor, dass personenbezogene Daten wie Adressen grundsätzlich nur dann an andere weitergegeben werden dürfen, wenn der Kunde vorher eingewilligt hat (Opt-in-Verfahren). Eine Ausnahme von diesem Verfahren bildet das so genannte Listenprivileg, welches das Bundesdatenschutzgesetz in § 28 Absatz 3 BDSG der Werbewirtschaft beim Versand von (Papier-)Werbung bereits vor der letzten Novellierung einräumte. Das Listenprivileg erlaubt die Übermittlung oder Nutzung von Daten, sofern es sich um listenmäßig zusammengefasste personenbezogene Daten über Angehörige einer Personengruppe handelt, die sich auf den Beruf, Namen, Titel und akademischen Grad, die Anschrift, das Geburtsjahr sowie die Angabe über die Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe (zum Beispiel männliche Studienanfänger unter 25 Jahren in Berlin) beschränken und dabei kein überwiegendes schutzwürdiges Interesse des Betroffenen verletzt wird.

Neu eingeführt wurde mit der letzten Novellierung des Bundesdatenschutzgesetzes die Regelung, dass Betroffene über die Herkunft ihrer Adressdaten auf dem Werbemittel mit Klarnamen und in drucktechnisch deutlicher Gestaltung informiert werden müssen (vergleiche § 28 Absatz 3 Satz 4 BDSG). Die Verwendung von Listendaten ist demnach erlaubt, wenn dies für die Bewerbung eigener Angebote der verantwortlichen Stelle erforderlich ist.

Mit der letzten Novellierung des Bundesdatenschutzgesetzes sind zudem einige Tatbestände hinzugekommen, die die Werbung für eigene Angebote mit zuvor erhobenen personenbezogenen Daten erleichtern. Die datenerhebende Stelle muss hierfür diese Listendaten beim Verbraucher im Rahmen des Vertragsschlusses beziehungsweise im Rahmen einer Anfrage als Interessent erhoben haben. Ergänzend können die Listendaten auch aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben worden sein. Um Profile für eine individualisierte Werbung erstellen zu können, darf die verantwortliche Stelle für die Bewerbung eigener Angebote zu den Listendaten weitere Daten hinzufügen, wenn diese personenbezogenen Daten zuvor ebenfalls rechtmäßig erhoben wurden.

Einzelne Fallgestaltungen sehen wie folgt aus:

So genanntes Lettershop-Verfahren

Unternehmen nutzen zur Neukundengewinnung Kundendaten, die von anderen Unternehmen für Werbezwecke vermietet werden. In diesem Fall beauftragt die verantwortliche Stelle – das Unternehmen, das Kundendaten etwa im Rahmen einer Geschäftsbeziehung erworben hat – einen Dienstleister mit der Nutzung seiner Kundendaten zur Erstellung eines Werbeschreibens. Das zu versendende Werbematerial wird dann von dem Unternehmen zur Verfügung gestellt, das die Daten zur Neukundengewinnung nutzen möchte.

Das dargestellte Verfahren ist mit den Vorgaben des Bundesdatenschutzgesetzes vereinbar, wenn das Unternehmen (verantwortliche Stelle), welches seine erworbenen Kundendaten für die Bewerbung von Produkten oder Dienstleistungen anderer Unternehmen zur Verfügung gestellt hat, für den Empfänger eindeutig erkennbar ist. Dies ist der Fall, wenn die Nennung des Unternehmens im Klartext erfolgt und der Empfänger so das Unternehmen ohne Zweifel und mit seinen Kenntnissen und Möglichkeiten identifizieren kann.

Übermittlung von Kundendaten (Kauf oder Tausch)

Beim Kauf oder Tausch von Kundendaten findet eine Übermittlung der Kundendaten von einem zu einem anderen Unternehmen statt. Das empfangende Unternehmen erhält die Kundendaten zur eigenen Verwendung und kann diese fortan für eigene werbliche Zwecke nutzen. Erfolgte die Übermittlung der Kundendaten ohne vorherige Einwilligung der Kunden ist der Vorgang nur dann rechtlich zulässig, wenn die gesetzlichen Informations-, Dokumentations- und Transparenzpflichten eingehalten werden.

Die gesetzliche Informationspflicht ist eingehalten, wenn der Kunde bei der Datenerhebung auf den Verwendungszweck eines Kaufs oder Tausches der erhobenen Kundendaten hingewiesen wurde. Zu beachten ist zudem, dass ein Kauf oder Tausch nur innerhalb der Gruppe möglich ist, die dem Kunden bei der Datenerhebung genannt wurde. Der gesetzlichen Dokumentationspflicht wird entsprochen, wenn die übermittelnde Stelle für den Zeitraum von zwei Jahren den Empfänger der Kundendaten speichert. Gleichzeitig muss der Empfänger der Kundendaten den Übermittler und den zulässigen Verwendungszweck für ebenfalls mindestens zwei Jahre speichern.

Ebenso wie im oben genannten Lettershop-Verfahren muss gegenüber dem Empfänger der Werbung die Quelle der Adresswerbung genannt werden. Ausfluss der gesetzlichen Transparenzpflicht ist zudem, dass gegenüber dem Empfänger der Werbung das Unternehmen zu benennen ist, welches erstmals die Kundendaten erhoben hat.

Die Übermittlung von Kundendaten zum Zwecke der Werbung ist somit letztlich, wie oben bereits dargestellt, auf die so genannten Listendaten begrenzt. Will ein Unternehmen darüber hinausgehende Daten übermitteln, muss eine Einwilligung des Betroffenen vorliegen.

Weitere Sonderfälle

Mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 wurden zwei weitere Sonderfälle gesetzlich für zulässig erklärt. Hierzu gehört die Nutzung und Übermittlung von Listendaten zur Bewerbung von Produkten und Dienstleistungen im gewerblichen Bereich. Allerdings erstreckt sich die gesetzliche Privilegierung auch auf Funktionsträger in Unternehmen (zum Beispiel „Abteilungsleiter Einkauf“). Abgrenzungsmerkmal ist demnach, dass die Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen erfolgen muss. Zudem darf nicht die Privatadresse, sondern es muss die berufliche Anschrift des Betroffenen verwendet werden. Fallen beide Adressen zusammen, kann trotzdem von der gesetzlichen Privilegierung Gebrauch gemacht werden.

Die Ausnahmeregelung für den gewerblichen Bereich erfasst sowohl die Vermietung von Listendaten als auch den Kauf oder Tausch der Daten. Gegenüber den oben genannten Regelungen besteht beim Vorliegen einer gewerblichen Ansprache keine Pflicht, die ursprüngliche Quelle der Daten offenzulegen. Auch die dargestellten Dokumentationspflichten müssen nicht eingehalten werden. Zudem ist für das werbende Unternehmen auch ein Rückgriff auf allgemein zugängliche Quellen zulässig. Die Adressdaten können somit beispielsweise auch über das Internet unmittelbar erhoben werden.

Eine weitere Ausnahme bei der Verwendung von Listendaten gilt, wenn steuerbegünstigte Organisationen für Spenden werben wollen. Auch in diesem Fall bedarf es keiner Angabe der Quelle, bei der erstmals die Daten erhoben wurden.

2.3.7 Spannungsfeld Datenschutz und Wettbewerbsbedingungen am Beispiel sozialer Netzwerke

Eine große datenschutzrechtliche Herausforderung im Internet sind inzwischen die sozialen Netzwerke, die in jüngerer Zeit die Nutzung des Internets zunehmend prägen. Betreiber sozialer Netzwerke haben ihren Sitz derzeit sowohl außerhalb des europäischen Wirtschaftsraums als auch innerhalb. Es stellen sich daher zunächst die grundsätzlichen Fragen der Anwendbarkeit und Durchsetzbarkeit nationalen oder aber europäischen Datenschutzrechts.[282]

Bei sozialen Netzwerken konnte festgestellt werden, dass besonders bei Änderungen des angebotenen Dienstes unterschiedliche datenschutzrechtliche Regelungen zur Anwendung kommen. Nach europäischem Datenschutzrecht muss beispielsweise jede Änderung eines Diensteangebots, bei der personenbezogene Daten betroffen sind, vom Nutzer bestätigt werden. Das umgekehrte Verfahren (so genanntes Opt-out) wird in den USA angewendet. Dieses führt zu weniger Rückläufern und ermöglicht damit eine stärkere Durchsetzung des eigenen Angebotes auf dem Markt.[283]

Hinzu kommt, dass derzeit Nutzerinnen und Nutzer vor der Eröffnung eines Kontos bei sozialen Netzwerken nicht in vergleichbar gut verständlicher Form über die Möglichkeiten der Betreiber, Daten zu verwenden, informiert werden. Zwar gibt es beispielsweise bei Facebook zahlreiche differenzierte Möglichkeiten, unter den Konto- oder Privatsphäre-Einstellungen den Zugriff auf Daten durch Dritte einzuschränken. Aber auf diese Möglichkeiten wird der Nutzer bei Einrichtung des Kontos nicht hingewiesen. Hier ist die datenschutzrechtliche Gefährdung höher als bei einer Opt-out-Lösung, bei der der Nutzer bei Kontoeröffnung über die Möglichkeit der Einstellungen informiert wird. Eine zusätzliche und besonders brisante Dimension kommt dann noch hinzu, wenn die Datenbestände sozialer Netzwerke mit anderen Kommunikationsformen datenmäßig miteinander kombiniert werden (etwa zwischen Facebook und Skype), ohne dass sich die Nutzer dessen bewusst wären.

2.3.8 Datenschutz als Standortfaktor

Datenschutz ist angesichts der internationalen Reichweite für viele Dienste ein wesentliches Wettbewerbselement und damit auch ein Standortfaktor einer innovativen und dynamischen Internetwirtschaft in Deutschland. Dabei bestehen hier durchaus zwei gegensätzliche Argumentationen:

Vertreten wird die Auffassung, striktere Datenschutzregeln seien hinderlich oder jedenfalls kostentreibend, wenn es darum gehe, mit neuen Diensten Marktanteile zu gewinnen. Für Unternehmen, die im internationalen Wettbewerb stehen, könne ein niedrigeres Datenschutzniveau sowohl zu einer Vereinfachung der Produktgestaltung als auch zu einer Erleichterung bei den Kosten führen.

Auf der anderen Seite wird vertreten, ein hohes Sicherheits- und Datenschutzniveau könne durch zusätzliches Kundenvertrauen zu einem positiven Unterscheidungsmerkmal im Wettbewerb werden. Wie bereits festgestellt, besteht durchaus ein Bewusstsein für die Relevanz hoher Sicherheits- und Datenschutzstandards und damit eine Nachfrage nach entsprechend ausgestalteten Produkten. Gelingt es also, ohne relevante Einbußen der sonstigen Wettbewerbsfähigkeit, hier ein Mehr gegenüber internationalen Diensten anzubieten, kann das hohe deutsche Schutzniveau auch als Standortvorteil verstanden und positioniert werden.

Von in Deutschland tätigen Unternehmen wird der Datenschutz aber auch deswegen zunehmend als negativer

[282] Vgl. die Darstellung in Kapitel 2.1.9.

[283] Vgl. Schriftliche Stellungnahme von Lars Hinrichs im Rahmen der Öffentlichen Anhörung „Auswirkungen der Digitalisierung auf unsere Gesellschaft – Bestandsaufnahme, Zukunftsaussichten“ der Enquete-Kommission Internet und Digitale Gesellschaft des Deutschen Bundestages am 5. Juli 2010. A.-Drs. 17(24)004-D, online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/2010/Sitzungen/20100705/A-Drs__17_24_004-D_-_Stellungnahme_Hinrichs.pdf

Standortfaktor wahrgenommen, weil sowohl die föderale Struktur der Datenschutzaufsicht als auch die Vielzahl bereichsspezifischer Regelungen eine einheitliche Anwendung und Auslegung innerhalb Deutschlands erschweren.

So hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder festgestellt: „Eine Vielzahl von Spezialregelungen, die das Bundesdatenschutzgesetz (BDSG) ganz oder teilweise überlagern und verdrängen, haben das Recht für Anwenderinnen und Anwender wie Betroffene unübersichtlich und unverständlich gemacht.“[284]

2.3.9 Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft

Staatliche Aufsicht ist unverzichtbar, gleichzeitig muss man aber anerkennen, dass sie systembedingt auch an Grenzen stößt. Selbst bei großer Sachnähe und einer hinreichenden personellen Ausstattung werden sich Behörden schwer tun, alle sich ständig wandelnden Phänomene im Internet in ihrer technischen Komplexität und Dynamik wirksam zu erfassen und eine hinreichende Aufsicht zu gewährleisten. Schließlich ergibt sich angesichts der Vielzahl der im Netz angebotenen Dienste unweigerlich ein Ressourcenproblem, das eine effektive, hinreichend enge Kontrolle der tatsächlichen Praxis bei den verantwortlichen Stellen erschwert.

Diese potenziellen Defizite staatlicher Aufsicht könnten durch eine Einbindung der Unternehmen in die Festsetzung und Durchsetzung von Datenschutzstandards ausgeglichen werden.[285]

Darüber hinaus können Selbstverpflichtungen der Internetwirtschaft in Zukunft auch im Datenschutz eine wichtige Ergänzung zu gesetzlichen Vorgaben darstellen. Gerade in einem sich schnell wandelnden Technikumfeld, aus dem sich ständig neue Geschäftsmodelle entwickeln, kann mit diesem Instrument flexibel auf Veränderungen reagiert und auf spezielle Bedürfnisse in einzelnen Anwendungsfällen eingegangen werden. Während mit der Gesetzgebung abstrakt-generelle Wertungen und Vorgaben von einer gewissen Nachhaltigkeit geschaffen werden müssen, kann mit Selbstverpflichtungen kurzfristiger und detaillierter eingegriffen werden, um auf Entwicklungen in einzelnen Geschäftsfeldern zu reagieren.

Dabei sind verschiedene formale und inhaltliche Ausgestaltungen denkbar, die von einseitigen Verpflichtungserklärungen der Verantwortlichen bis zu einer gesetzlich eingebundenen regulierten Selbstregulierung gehen. Bereits im geltenden Bundesdatenschutzgesetz stellt § 38a einen rechtlichen Anknüpfungspunkt dar, über den Selbstverpflichtungen in den gesetzlichen Rahmen integriert werden können. Bislang wurde dieses Instrument kaum genutzt. Jüngste Beispiele wie der Datenschutz-Kodex für Geodatendienste[286] könnten jedoch der Anfang einer deutlich intensiveren Nutzung dieses Regulierungsinstruments sein. Diese Entwicklung ist zu beobachten und gegebenenfalls durch entsprechende Ergänzung des Rechtsrahmens zu fördern. Auch die EU-Kommission hat in ihrer Mitteilung angekündigt, „Möglichkeiten zur verstärkten Förderung von Initiativen zur Selbstregulierung zu prüfen, darunter die aktive Förderung von Verhaltenskodizes“[287].

So wird zurzeit auf europäischer Ebene auch die Einführung von Selbstregulierungsmechanismen für angemessene Formen der Datenerhebung und -verwendung im Zusammenhang mit Onlinewerbung erörtert. Das könnte ein wichtiger Schritt sein, um auch in diesem Bereich zu mehr Transparenz und Selbstbestimmungsmöglichkeiten für die Nutzerinnen und Nutzer zu kommen. Denn klare Kennzeichnungen von verpflichtungskonformen Angeboten bieten dem Nutzer zusätzliche Transparenz und einfache Orientierungsmöglichkeit.[288]

2.3.10 Übertragbarkeit der regulierten Selbstregulierung auf den Bereich des Datenschutzes

Insbesondere im Jugendmedienschutz hat sich neben staatlicher Regulierung und reiner Selbstregulierung eine Form der so genannten regulierten Selbstregulierung beziehungsweise Co-Regulierung entwickelt. Sie ist dadurch gekennzeichnet, dass die staatliche Hand einen gesetzlichen Rahmen schafft, innerhalb dessen die Selbstkontrolle der Wirtschaft in eigener Verantwortung die Ausgestaltung und Anwendung von Verhaltensgrundsätzen organisieren kann. Sie unterliegt dabei aber wiederum einer übergeordneten Erfolgskontrolle durch die staatliche Hand, die im Falle von Fehlentwicklungen oder Verstößen gegen den vorgegebenen Rahmen ihrerseits durchgreifen kann. Der Erfolg dieses Modells im Jugendmedienschutz hängt wesentlich damit zusammen, dass es in diesem Bereich einen Beurteilungsspielraum bei der Bewertung der der Kontrolle unterliegenden Medieninhalte gibt. Für die Einschätzung der potenziellen Entwicklungsbeeinträchtigung und der damit verbundenen Altersklassifizierung existieren keine gesetzlichen Vorgaben, sodass diese rein tatsächliche Beurteilung am besten

[284] Vgl. Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 5. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapier Broschuere.pdf?__blob=publicationFile

[285] Die Fraktion BÜNDNIS 90/DIE GRÜNEN hat gegen die Textfassung dieses Absatzes gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.3.4).

[286] BITKOM. Datenschutzkodex für Geodatendienste – Entwurf. Dezember 2010. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/rote_linie_kodex.pdf?__blob=publicationFile

[287] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4. November 2010. KOM (2010) 609, Kapitel 2.2.5 (S.14).

[288] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben gegen diese Textfassung des Kapitels 2.3.9 *Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft* gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.3.3).

von möglichst sachnahen Personen durchgeführt werden sollte.

Einen solchen Beurteilungsspielraum kennt das viel stärker von Rechts- als von Tatsachenfragen geprägte Datenschutzrecht allerdings nicht. Hier bestehen bereits aus verfassungsrechtlichen Gründen durchgehende gesetzliche Regelungen, deren Auslegung zwar im Einzelfall schwierig und auch streitig sein kann, die aber trotzdem mit einem vollumfänglichen Geltungsanspruch ausgestattet sind. Es erscheint daher fraglich, ob es im Datenschutz einen dem Jugendmedienschutz vergleichbaren Spielraum für die sachliche Ausfüllung von Tatbestandselementen gibt, die das Modell einer regulierten Selbstregulierung tragen könnten. Es liegt näher, dass sich in diesem Bereich angesichts des vollumfänglichen Geltungsanspruchs staatlicher Regulierung nur ein Nebeneinander, aber eben kein ineinander verwobenes Miteinander von staatlicher Regulierung einerseits und Selbstregulierung der Wirtschaft andererseits entwickeln kann.

2.3.11 Schadensersatzansprüche im Datenschutzrecht

Bei der Verletzung des Rechts auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG tritt selten ein materieller, sondern ein immaterieller Schaden ein. Dem Betroffenen steht nach § 7 BDSG (in Umsetzung von Artikel 23 DSRL) gegenüber der verantwortlichen (nicht-öffentlichen und öffentlichen) Stelle ein Schadensersatzanspruch zu, sofern personenbezogene Daten unzulässig oder unrichtig erhoben, verarbeitet oder genutzt wurden und ein Schaden entstanden ist. Die fehlerhafte Datenverarbeitung muss ursächlich für den Schaden geworden und im Sinne von § 276 BGB schuldhaft, das heißt durch vorsätzlichen oder fahrlässigen Umgang erfolgt sein.[289] Dabei wird zunächst schuldhaftes Handeln durch die verantwortliche Stelle unterstellt, die nach § 7 Satz 2 BDSG jedoch den Entlastungsbeweis führen kann und damit die Möglichkeit zur Exkulpation hat. Der zugefügte Schaden muss eine materielle Beeinträchtigung des Betroffenen zur Folge haben, das heißt ein so genannter Vermögensschaden muss vorliegen, der konkret beziffert werden muss.

Bei automatisierter Datenverarbeitung durch öffentliche Stellen besteht für die Betroffenen im Falle unzulässiger oder unrichtiger Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten nach § 8 Absatz 1 BDSG (ebenfalls in Umsetzung von Artikel 23 DSRL) ein Schadensersatzanspruch. Diese verschuldensunabhängige Gefährdungshaftung soll die „typische Automationsgefährdung“ abdecken, also Schäden, die durch automatisierte Verfahren eingetreten sind.[290] Es besteht keine Exkulpationsmöglichkeit für die datenverarbeitende Stelle. Ersetzt werden nicht nur materielle, sondern auch immaterielle Schäden, sofern eine schwere Verletzung des Persönlichkeitsrechts geltend gemacht werden kann.

[289] Vgl. Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 7, 8.
[290] Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 8 Rn. 9.

Das Verhältnis der gesetzlichen Ansprüche nach §§ 7, 8 BDSG zu dem deliktischen Schadensersatzanspruch nach § 823 BGB ist bisher jedoch noch umstritten. Hierzu werden verschiedene Auffassungen vertreten, die jedoch im Ergebnis mehrheitlich auch einen Ersatz immaterieller Schäden bei einer schwerwiegenden Verletzung aufgrund eines unzulässigen oder unrichtigen Datenumgangs annehmen.[291] Hierzu gibt es jedoch noch keine Rechtsprechung.

Bei öffentlichen Stellen kann sich eine über §§ 7, 8 BDSG hinausgehende Haftung im Rahmen hoheitlicher Tätigkeit nach Artikel 34 GG in Verbindung mit § 839 BGB oder im fiskalischen Bereich aufgrund vertraglicher oder deliktischer Haftung nach §§ 31, 89 beziehungsweise § 831 BGB ergeben.[292] Darüber hinaus können Schadensersatzansprüche gemäß § 280 BGB wegen schuldhaft rechtswidriger oder missbräuchlicher Datenverarbeitung aus vorvertraglicher beziehungsweise vertraglicher Haftung bestehen.[293]

Der Nutzen von Schadensersatzansprüchen im Datenschutzrecht ist in der Praxis dadurch beschränkt, dass es oftmals schwierig ist, einen konkreten ersatzfähigen Schaden aufzuzeigen. In vielen Fällen kann ein Schaden gar nicht beziffert werden, weil keine konkrete materielle Einbuße vorliegt. Immaterielle Schäden sind wiederum im deutschen Recht generell nur unter sehr engen Einschränkungen ersatzfähig. Schließlich kann aufgrund der technischen Zusammenhänge auch der Nachweis der Kausalität für den Schadenseintritt Schwierigkeiten bereiten.

2.3.12 Beschäftigtendatenschutz

Seit Jahrzehnten wird die Schaffung umfassender gesetzlicher Regelungen für den Arbeitnehmerdatenschutz diskutiert. Die christlich-liberale Koalition hat sich daher bereits im Koalitionsvertrag vom 26. Oktober 2009 für eine Erweiterung des Bundesdatenschutzgesetzes ausgesprochen. Denn gegenwärtig existieren nur wenige spezifische gesetzliche Vorschriften zum Schutz der personenbezogenen Daten von Beschäftigten. Für zahlreiche Fragen der Praxis zum Beschäftigtendatenschutz bestehen keine speziellen gesetzlichen Regelungen. Teilweise ergibt sich der rechtliche Rahmen für den Beschäftigtendatenschutz aus verschiedenen allgemeinen Gesetzen wie dem Bundesdatenschutzgesetz und dem Betriebsverfassungsgesetz. Daneben existiert eine Vielzahl an gerichtlichen Einzelfallentscheidungen, anhand derer wichtige Grundsätze für den Beschäftigtendatenschutz entwickelt worden sind. Jedoch sind insbesondere die gerichtlichen Entscheidungen für die betroffenen Beschäftigten teilweise nur schwer zu erschließen.

[291] Vgl. Kühling, Jürgen/Bohnen, Simon: Zur Zukunft des Datenschutzrechts. JZ 2010, 600 (609).
[292] Vgl. Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 17.
[293] Vgl. Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 18.

Durch die Erweiterung des Bundesdatenschutzgesetzes[294] soll die Rechtssicherheit für Arbeitgeber und Beschäftigte erhöht werden. So sollen einerseits die Beschäftigten vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten geschützt werden, andererseits soll das Informationsinteresse des Arbeitgebers beachtet werden. Beides dient dazu, ein vertrauensvolles Arbeitsklima zwischen Arbeitgebern und Beschäftigten am Arbeitsplatz zu unterstützen.

Es sollen für Zwecke des Beschäftigungsverhältnisses nur solche Daten verarbeitet werden dürfen, die für dieses Verhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Beschäftigungsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante Gesundheitszustände beziehen, sollen (zukünftig) ausgeschlossen sein. Mit den Neuregelungen sollen Mitarbeiter an ihrem Arbeitsplatz zudem wirksam vor Bespitzelungen geschützt und gleichzeitig den Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand gegeben werden.[295] [296]

2.3.13 Probleme der föderalen Aufsichtsstruktur

In ähnlicher Weise wie im internationalen Bereich gibt es auch im Inland vielfältige Situationen, in denen bestehende Rechtsvorschriften unterschiedlich angewendet und ausgelegt werden. Von Vorteil ist zwar, dass der Datenschutz im nicht-öffentlichen Bereich maßgeblich durch das Bundesdatenschutzgesetz geprägt wird und damit bundeseinheitliche Vorgaben bestehen.

Durch die weitgehende Zuständigkeit der Bundesländer für die Datenschutzaufsicht kommt es allerdings häufig zu einer unterschiedlich strikten Anwendung und teils weiteren, teils engeren Auslegung vor allem von eher unbestimmten Regelungen. Manche verantwortliche Stellen sind zudem gleich mehreren Aufsichtsbehörden unterworfen, insbesondere wenn die Aufsicht teils dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, teils der Landesdatenschutzaufsicht obliegt.

Andererseits wird vorgetragen, dass der Erfolg der deutschen Datenschutzaufsicht wesentlich auf den „föderalen Wettbewerb“ und die Herausbildung von Best Practices zurückzuführen ist. Zudem kann darauf verwiesen werden, dass erst die dezentrale Struktur eine flächendeckende Aufsicht „vor Ort“ zu gewährleisten im Stande ist.

Eine Abstimmung der Aufsichtsbehörden erfolgt weitgehend informell, insbesondere in Form von Konferenzen (vor allem für den öffentlichen Bereich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Düsseldorfer Kreis für den nicht-öffentlichen Bereich). Die Konferenzen und die daraus resultierenden Veröffentlichungen geben Orientierung, können aber formal keine unmittelbaren normativen Wirkungen entfalten und die bestehenden Rechtsunsicherheiten nicht gänzlich auflösen.

3 Handlungsempfehlungen

3.1 Einleitung

Die anhaltenden Veränderungen in der Informationstechnologie ziehen notwendigerweise Veränderungen in nahezu allen Lebensbereichen und damit auch bei den dafür geschaffenen Datenschutzbestimmungen nach sich. Seit ihren Anfängen haben sich die Anforderungen an den Schutz personenbezogener Daten laufend stark verändert. Nicht nur, aber besonders auch aufgrund des Erfolges des Internets (zum Beispiel schnell steigende Rechner- und Leitungskapazitäten, Ausweitung und fortlaufende Verbesserung von Software sowie von mobilen Anwendungen) und der zunehmenden Vernetzung in den Diensten und Anwendungen des Web 2.0 bis hin zu einer praktisch allgegenwärtigen rechnergestützten Informationsverarbeitung (Ubiquitous Computing) haben sich die Herausforderungen an den Datenschutz in den letzten Jahren potenziert.

Sowohl der nationale als auch der europäische Gesetzgeber sind diesem rasanten technischen und kulturellen Wandel in Teilen gefolgt. Seit den 1970er Jahren wurden daher die datenschutzrechtlichen Bestimmungen immer wieder angepasst und fortgeschrieben. Dies hat dazu geführt, dass in Deutschland mittlerweile vergleichsweise sehr differenzierte Aussagen sowohl zu den Inhalten als auch zu den Grenzen des Datenschutzes existieren. Obwohl bereits mehrere Anläufe zu einer grundsätzlichen Modernisierung auf nationaler und auf europäischer Ebene unternommen wurden, konnten sie bisher allerdings noch nicht erfolgreich abgeschlossen werden. Aufgrund des technologischen Fortschritts steht der Gesetzgeber jedoch weiterhin unter einem ständigen Veränderungs- und Nachbesserungsdruck, ein Leerlaufen bestehender Regelungen zu vermeiden. Hinzu kommt, dass auch die zu schützenden Werte in einer digitalen Gesellschaft in dem Maße weiter an Wert und Bedeutung zunehmen werden, in dem diese durch den technologischen Wandel unter Druck geraten. Viele datenschutzrechtliche Grundprinzipien beruhen noch immer auf dem Schutzmodell der 1970er Jahre. Ihr Fortbestand und ihre Anwendbarkeit auf die digitale Gesellschaft werden daher vor dem Hintergrund der großen Anzahl neu aufgeworfener Fragen und Probleme kritisch diskutiert.

Auch wenn der Datenschutz einem gesellschaftlichen Wandel und somit auch unterschiedlichen „Strömungen“ unterliegt, sind sich die Mitglieder der Enquete-Kommission einig, dass das Grundrecht auf informationelle Selbstbestimmung nach wie vor Geltung beansprucht und

[294] Gesetzesentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes. Bundestagsdrucksache 17/4230 vom 15. Dezember 2010.

[295] Gesetzesentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes. Bundestagsdrucksache 17/4230 vom 15. Dezember 2010, S. 12.

[296] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg haben gegen diese Textfassung des Kapitels 2.3.12 *Beschäftigtendatenschutz* gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.1.3.5).

dieser Anspruch auch nicht aufgegeben werden darf. Es ist ein Grundelement einer freien und demokratischen Kommunikationsverfassung und damit elementare Funktionsbedingung eines freiheitlich-demokratischen Gemeinwesens, das auf die Handlungs- und Mitwirkungsfähigkeit seiner Bürger angewiesen ist. Es vermag über die mittelbare Drittwirkung auf das Privatrecht einzuwirken und kann den Gesetzgeber in seinem objektiv-schutzrechtlichen Gehalt zu effektiven Schutzmaßnahmen verpflichten. In der digitalen Gesellschaft ist ihm und seiner adäquaten Ausgestaltung ein noch höherer Wert beizumessen.

Gesellschaftliche Veränderungen hinsichtlich der Wahrnehmung des Umgangs mit (personenbezogenen) Daten im Internet sind in Deutschland spätestens seit der breiten öffentlichen Diskussion über Anbieter von Geodatendiensten im Jahr 2010 erkennbar. Zwar entzündete sich diese öffentliche Diskussion aus datenschutzrechtlicher Sicht an einem wenig geeigneten Thema, weil es sich zumindest bei den bildmäßig erfassten Hausfassaden um überwiegend öffentlich wahrnehmbare Objekte handelt, bei denen bereits der Personenbezug streitig ist. Dennoch kommt darin eine zunehmende Besorgnis gegenüber den möglichen Folgen des technologischen Fortschritts im Internet zum Ausdruck.

Die gesellschaftliche Reaktion auf die genannten Veränderungen ist in Deutschland deutlich. In Umfragen[297] wünscht sich regelmäßig eine deutliche Mehrheit der Bundesbürger einen verbesserten Schutz ihrer Daten. Denn viele Bürgerinnen und Bürger fürchten den Missbrauch ihrer personenbezogenen Daten, besonders bei der Nutzung des Internets.

Beispiele wie Google Street View oder der vergleichbare Dienst Microsoft Streetside, aber auch zum Beispiel die Möglichkeiten, in sozialen Netzwerken Fotos und Adressbücher (und damit Daten Dritter) einzustellen, führen dazu, dass es zunehmend schwerer wird, sich einer ungewollten Erhebung und Weiterverarbeitung personenbezogener Daten im Internet gänzlich zu entziehen. Hierdurch kann auch eine Verschiebung der „Handlungslast“ auf die Betroffenen eintreten. Dies gilt insbesondere für den Fall, dass diese nicht mit einer Veröffentlichung ihrer personenbezogenen Daten einverstanden waren. Häufig müssen sie nun von sich aus aktiv tätig werden, um entstandene digitale Spuren zu entfernen. Doch Besorgnis und Zutrauen liegen nicht weit auseinander. So werden viele der mit dem Schlagwort Web 2.0 umschriebenen neuen Anwendungen und Dienste bereits nach kurzer Zeit ausgiebig auch von Nutzerinnen und Nutzern in Deutschland in Anspruch genommen. Dies legt die Vermutung nahe, dass die möglichen Folgen einer solchen Nutzung für das eigene oder das Recht anderer auf informationelle Selbstbestimmung oftmals vernachlässigt werden oder aber bei einer Nutzen-Risiko-Abwägung der Nutzen zu überwiegen scheint. Ein Beispiel hierfür stellen einmal mehr die sozialen Netzwerke als wesentlicher Kern des Web 2.0 dar. Schon die ersten Formen wurden intensiv von mehreren Millionen Menschen unterschiedlichen Alters weltweit genutzt. Bis heute haben sie nichts an ihrer Attraktivität eingebüßt. Im Gegenteil: Rasante gesellschaftliche und auch politische Veränderungen lassen sich weltweit unter anderem auch auf soziale Netzwerke als Kommunikationsinstrument zurückführen. Die auf der Mitteilung und Eingabe von personenbezogenen Daten (zum Beispiel Lebensweisen, Gewohnheiten und Präferenzen) basierenden Netzwerke haben sich jedoch auch schon als Bumerang für manchen Nutzer erwiesen. Dies gilt insbesondere, wenn Dritte sich unberechtigt Zugang zu schützenswerten Daten verschaffen konnten oder sich bereits eingestellte personenbezogene Daten nachträglich nicht mehr „zurückholen“ ließen. Besonderen Aufwand erfordern auch die datenschutzrechtlichen Grundeinstellungen für die Nutzerinnen und Nutzer. So gelten pseudonyme Nutzungen bei Facebook als mit den AGB unvereinbar. Ein Teil der eingestellten Daten und Informationen steht zunächst allen Mitgliedern und teilweise auch der Öffentlichkeit zur Verfügung, wenn die Nutzer nicht von sich aus Veränderungen an den Einstellungen vornehmen.

In der digitalen Gesellschaft zeichnet sich eine Entwicklung dahingehend ab, dass Dienste oder Anwendungen, die mit einer Individualisierung einhergehen, als attraktiver wahrgenommen werden. Eine solche Individualisierung setzt die Eingabe oder Bereitstellung personenbezogener Daten durch den Nutzer selbst voraus. Oft erheben und verarbeiten die Anbieter vom Nutzer zunächst unbemerkt Daten, um individualisierte Dienste zur Verfügung zu stellen. Der Nutzer und sein Verhalten werden damit zum Mittelpunkt. Bei vielen Diensten und Anwendungen werden aber auch personenbezogene Daten erhoben, obwohl dies nicht unmittelbar zu einem erkennbaren Mehrwert für den Nutzer führt.

Für die Nutzerinnen und Nutzer hat all dies zur Folge, dass sie sich fortlaufend an die veränderten Gegebenheiten anpassen müssen, wollen sie neue Dienste beziehungsweise die Weiterentwicklung bestehender Dienste weiterhin nutzen und dabei wirksam von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen. Hierzu bedarf es nicht nur des notwendigen Wissens und damit eines entsprechend kompetenten Umgangs mit dem Medium Internet, sondern auch einer permanenten Aktualisierung und Erweiterung des Wissens über die Funktionsweisen und Auswirkungen der vorhandenen und benutzten Anwendungen und Dienste.

Auch für die Anbieter steigt durch diese Ausrichtung ihrer Geschäftstätigkeit die Verantwortung im Umgang mit den Daten und Informationen ihrer Kundinnen und Kunden. Hinreichend konkrete Vorgaben für die Einhaltung

---

[297] Siehe u. a. TNS Infratest im Auftrag von Microsoft: Studienergebnisse „Datenschutz im digitalen Zeitalter - Trends und Spannungsfelder“. Mai/Juni 2011. http://download.microsoft.com/download/2/0/B/20BE3B2A-7563-40C7-9BD6-9CF5E2AEF5ED/Datenschutzstudie_2011_Microsoft.pdf; Institut für Demoskopie Allensbach im Auftrag der SCHUFA Holding AG: Die Einstellung der Deutschen zum Thema Datenschutz. Studie von September 2010 (siehe auch unter http://www.schufa.de/de/private/presse/aktuellepressemitteilungen/2010/100929.jsp); BITKOM: Datenschutz im Internet. Juni 2010. http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf

und Umsetzung datenschutzrechtlicher Bestimmungen stärken dabei sowohl das Vertrauen der Nutzer als auch die Rechtssicherheit der Anbieter. In diesem Zusammenhang sollte der Datenschutz nicht als Grenze technologischer Entwicklungen gesehen, sondern auch als Chance zur Erhöhung der Akzeptanz neuer Technologien ausgestaltet werden.

Die Beratungen in der Enquete-Kommission zum Thema Datenschutz und Persönlichkeitsrechte haben gezeigt, dass es einen breiten Konsens über die Grundprinzipien, Ziele und Werte des Datenschutzes gibt. Alle Mitglieder der Enquete-Kommission heben hervor, dass Datenschutz und eine Gewährleistung des Grundrechts auf informationelle Selbstbestimmung Akzeptanz und Vertrauen schaffen. Beide sind unabdingbar für den technologischen Fortschritt in einer digitalen Gesellschaft.

Vor diesem Hintergrund gibt die Enquete-Kommission nachfolgende Handlungsempfehlungen:

3.2 Vorgaben für nationalen, europäischen und internationalen Datenschutz

Die Zukunft des Datenschutzes liegt längst nicht mehr allein auf nationaler, sondern auf europäischer und insbesondere auf internationaler Ebene. Die Enquete-Kommission begrüßt daher grundsätzlich das Ziel der Mitteilung der EU-Kommission vom 4. November 2010[298], das bestehende Datenschutzrecht auf europäischer Ebene zu novellieren und zu modernisieren, um es so an die neuen technischen Anforderungen des digitalen Zeitalters anzupassen. Insbesondere die Zielsetzung der EU-Kommission, die Rechte des Einzelnen zu stärken, den Verwaltungsaufwand für die Unternehmen zu verringern und ein einheitlich hohes Schutzniveau in und außerhalb der EU zu gewährleisten, unterstützt die Enquete-Kommission grundsätzlich.

Aber auch die Anstrengungen der EU-Kommission, die Zusammenarbeit mit Drittstaaten und internationalen Organisationen, einschließlich der Vereinten Nationen, des Europarats und der OECD sowie internationaler Normungsorganisationen wie dem Europäischen Komitee für Normung (Comité Européen de Normalisation – CEN), der Internationalen Organisation für Normung (International Organization for Standardization – ISO), dem World Wide Web Consortium (W3C) und der Internet Engineering Task Force (IETF) zu verbessern, finden die Unterstützung durch die Enquete-Kommission. Aus Sicht der Enquete-Kommission sollte daher die Bundesregierung sowohl prüfen, ob sie ihre eigenen Anstrengungen in den vorgenannten Gremien im Hinblick auf den Datenschutz intensivieren kann als auch ob es der Anregung weiterer Verhandlungsmandate für die EU-Kommission bedarf.

[298] Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Gesamtkonzept für den Datenschutz in der Europäischen Union“, KOM (2010) 609, online abrufbar unter: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf

1. Die Enquete-Kommission sieht Handlungsbedarf darin, die Wettbewerbsposition deutscher Anbieter von Internetdiensten gegenüber ausländischen Mitbewerbern durch den Gesetzgeber weiter fortlaufend zu analysieren. Gerade im Bereich der sozialen Netzwerke halten sich ausländische Anbieter, die keinen Sitz in Deutschland haben, teilweise nicht an nationale datenschutzrechtliche Bestimmungen. Zugleich besteht auf nationaler Ebene ein Vollzugsdefizit, das geltende Recht auch wirksam gegenüber ausländischen Anbietern von Diensten umzusetzen, wenn diese über keinen inländischen Sitz verfügen. Die Enquete-Kommission regt daher eine kurzfristige Befassung des Deutschen Bundestags an, wie die Probleme des Anwendungsbereichs und bestehende Vollzugsdefizite zielgerichtet behoben werden können. Im Rahmen einer solchen Diskussion gibt die Enquete-Kommission zu bedenken, dass nationales Datenschutzrecht nicht immer bei weltweiten Angeboten angewendet werden kann.

2. Aus Sicht der Enquete-Kommission sollte die Bundesregierung prüfen, ob zukünftig bei international und europaweit tätigen Unternehmen mit mehreren Niederlassungen in Mitgliedstaaten der EU in Fragen des Datenschutzes im Internet eine stärkere Koordinierung der datenschutzrechtlichen Aufsicht sowohl auf europäischer wie auch nationaler Ebene, etwa durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, wahrgenommen werden sollte. Hierzu wäre die Schaffung eines verbindlichen Abstimmungsverfahrens erforderlich.

3. Aus Sicht der Enquete-Kommission ist es fraglich, ob die bisherigen nationalen und europäischen Regelungen zur Auftragsdatenverarbeitung für eine rechtssichere Teilnahme von Unternehmen am so genannten Cloud-Computing ausreichend sind. Im Zuge der Novellierung der Datenschutzrichtlinie sollten daher Regelungen geschaffen werden, die Unternehmen die Nutzung von Cloud-Computing und neue Entwicklungen in diesem Bereich ermöglichen. Diese Regelungen sollten gleichzeitig ein hohes Datenschutzniveau sicherstellen und damit die Belange der Nutzerinnen und Nutzer berücksichtigen sowie den Wirtschaftsstandort Europa stärken.

4. Aus Sicht der Enquete-Kommission muss ein novelliertes europäisches Datenschutzrecht der modernen Arbeitsweise international organisierter Konzerne stärker als bisher Rechnung tragen. Datenschutz und Datenaustausch in verbundenen Unternehmen müssen unter Beachtung des Rechts auf informationelle Selbstbestimmung rechtssicher und damit gegebenenfalls vereinfacht ausgestaltet werden.

5. Die Enquete-Kommission regt eine Prüfung auf europäischer Ebene an, ob dem Datenschutzrecht ein wettbewerbsschützender Charakter zugeschrieben werden kann. Schließlich könnte dies zu einer stärkeren gegenseitigen Kontrolle der Marktteilnehmer im nicht-

öffentlichen Bereich und somit zu einer besseren Durchsetzbarkeit des Datenschutzes führen.[299] [300]

3.3 Datenschutz als Standortfaktor

Die Einhaltung von datenschutzrechtlichen Bestimmungen und die Schaffung eines hohen Datenschutzniveaus könnten gerade im europäischen und internationalen Vergleich zu einem positiven Wirtschaftsfaktor und somit zu einem vermarktungsfähigen Alleinstellungsmerkmal werden. Diese dürfen daher nicht nur als möglicher Kostenfaktor gesehen werden. Das Bewusstsein der Nutzerinnen und Nutzer für datenschutzfreundliche Angebote muss jedoch weiter gestärkt werden, damit sie den Markt entsprechend mitgestalten.

Die Enquete-Kommission regt an, nationale und verstärkt auch internationale Initiativen für Datenschutz zusammenzufassen.

Nationale Initiativen könnten dabei unter einem Markenzeichen wie beispielsweise „Made in Germany" oder „Made in Europe" zusammengeführt werden, um so das hohe nationale Datenschutzniveau als Qualitätsmerkmal besser herausstellen und vermarkten zu können. Einen wichtigen Beitrag hierzu können freiwillige Gütesiegel und Audits, die auf verbindlichen Auditierungsverfahren beruhen und von unabhängiger Stelle angeboten und durchgeführt werden, leisten.

3.4 Einwilligung

Die Enquete-Kommission hat in ihrem Bericht herausgearbeitet, dass eine informierte und freiwillige Einwilligung des Einzelnen oft nicht stattfindet – und zwar aus unterschiedlichen Gründen. Darüber hinaus ist ein Überblick für die Nutzerinnen und Nutzer über bereits erteilte Einwilligungen nur schwer zu behalten.

Deshalb empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

1. die Informationspflichten so auszugestalten, dass die Informationen von der Art und vom Umfang her die Grundlage für informierte und freiwillige Einwilligungen bilden,
2. die im Jahr 2009 verabschiedete Regelung der elektronischen Einwilligung nach § 28 Absatz 3a BDSG in den Allgemeinen Teil des Bundesdatenschutzgesetzes unter § 4a BDSG zu übernehmen, damit ihr Anwendungsbereich sich nicht nur auf Werbeeinwilligungen, sondern auf alle elektronischen Einwilligungen erstreckt,
3. zu prüfen, ob es erforderlich erscheint, § 13 Absatz 2 TMG im Hinblick auf ein gesetzlich geregeltes Opt-in-Verfahren (bei dem Betroffene aktiv in die Datenerhebung und -verarbeitung einwilligen, zum Beispiel durch Ankreuzen oder Setzen eines Häkchens) zu konkretisieren und die Anforderungen technikneutral auszugestalten,
4. zu prüfen, ob eine zeitliche Befristung von Einwilligungen sinnvoll und zielführend ist und welche Konsequenzen sich hieraus für das bestehende Recht der Einwilligung ergeben könnten,
5. in Betracht zu ziehen, den Widerruf der Einwilligung im Bundesdatenschutzgesetz klarstellend zu regeln. Dies gilt insbesondere mit Blick auf die Weitergabe von Daten. Hier wird empfohlen, dass bereits der Widerruf bei der Stelle genügt, die erstmals die Daten erhoben und weitergegeben hat. Der Widerruf wäre durch diese Stelle an die weiteren Stellen weiterzureichen,
6. die in der E-Privacy-Richtlinie vorgesehenen Anforderungen an Information und Zustimmung bei der Platzierung von Cookies für einen wirksamen Schutz bei der Verarbeitung personenbezogener Daten durch den Gesetzgeber in deutsches Recht umzusetzen.[301]

3.5 AGB und Datenschutz

Insbesondere die in kurzem zeitlichen Abstand erfolgenden mehrfachen Änderungen der Datenschutzbestimmungen in AGB von Anbietern von Internetdiensten, darunter auch Anbieter sozialer Netzwerke, werfen rechtliche Fragen auf. Die Enquete-Kommission fordert, gesetzlich klarzustellen, dass Anbieter von Diensten verpflichtet sind, den rechtzeitigen Vorabzugang veränderter Datenschutzbestimmungen an alle Nutzerinnen und Nutzer sicherzustellen.

Auch wenn es Ziel aller Anbieter von Diensten sein sollte, den Nutzern Datenschutzinformationen in prägnanter und kurzer Form anzubieten, um so eine bewusste Kenntnisnahme deutlich zu erleichtern und das Vertrauen in netzbasierte Anwendungen und Transaktionen zu stärken, gelingt dies nur in den wenigsten Fällen. Nach wie vor müssen viele Nutzer zunächst umfangreiche, teilweise auch schwer verständliche und oft juristisch formulierte AGB zur Kenntnis nehmen.

Die Bundesregierung sollte daher prüfen,

1. ob die Möglichkeit besteht, leicht verständliche und nachvollziehbare Datenschutzerklärungen zu entwickeln, die für eine Vielzahl von Angeboten im Internet anwendbar sind. Damit könnte die Transparenz für die Nutzerinnen und Nutzer erhöht und eine erhebliche Vereinfachung für die betroffenen Unternehmen erzielt werden,

[299] Die Fraktionen CDU/CSU und FDP sowie die Sachverständigen Prof. Dr. Hubertus Gersdorf, Prof. Dieter Gorny, Dr. Wolf Osthaus und Dr. Bernhard Rohleder haben ein ergänzendes Sondervotum zum Kapitel 3.2 *Vorgaben für nationalen, europäischen und internationalen Datenschutz* abgegeben (siehe Kapitel 4.2.1.1).

[300] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel 3.2 *Vorgaben für nationalen, europäischen und internationalen Datenschutz* abgegeben (siehe Kapitel 4.2.2.1).

[301] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel 3.4 *Einwilligung* abgegeben (siehe Kapitel 4.2.2.2).

2. ob die Möglichkeit besteht, Verwender von Datenschutzerklärungen in AGB gesetzlich zu verpflichten, diese bereits auf der Startseite in kurzer und verständlicher Form zum Abruf bereitzuhalten.

3.6 Privacy by Design und Privacy by Default

Privacy by Design und Privacy by Default orientieren sich an den Vorgaben der Datenvermeidung und Datensparsamkeit und damit an den zentralen Leitlinien des Datenschutzrechts.

Elemente von Privacy by Design sind beispielsweise eine grundsätzliche Verschlüsselung von Daten oder die automatisierte Löschung von Daten nach Funktionserfüllung.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, das Prinzip Privacy by Design grundsätzlich als verpflichtende Vorgabe bei der Entwicklung und dem Einsatz neuer Technologien zu formulieren.

Der Grundsatz Privacy by Default gewährleistet, dass die Nutzerinnen und Nutzer bei der Reduzierung des Schutzniveaus von Diensten, Technologien und Anwendungen aktiv entscheiden müssten, welche Veränderungen des höchstmöglichen Schutzniveaus sie zulassen möchten.

Die Enquete-Kommission sieht im Prinzip des Privacy by Default eine wichtige Option zur Gestaltung von elektronischen Diensten und Anwendungen im Internet (zum Beispiel bei deutschen sozialen Netzwerken oder so genannten Location-based Services). Die Anwendung von datenschutzfreundlichen Voreinstellungen erscheint gerade angesichts der Vielfalt der einzelnen technischen Einstellungen vieler webbasierter Angebote und der oftmals nicht leicht erkennbaren Konsequenzen sinnvoll. Sie begrüßt daher, dass viele Anbieter von Diensten im Internet sich bereits freiwillig zu einer Umsetzung von Privacy by Default verpflichtet haben.

Die Enquete-Kommission regt an, die bereits bestehenden gesetzlichen Vorgaben der Datenvermeidung und Datensparsamkeit (vergleiche § 3a BDSG) mit dem Prinzip Privacy by Default gesetzlich zusammenzuführen.[302]

3.7 Verfallsdaten

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, die Diskussion um Verfallsdaten im Internet auf nationaler und europäischer Ebene weiter zu verfolgen, denn die Entwicklung von technischen Lösungen für ein Vergessen im Internet steht erst am Anfang. Die Enquete-Kommission sieht in der Initiative der Bundesregierung, mit Hilfe eines Ideenwettbewerbs entsprechende technische Möglichkeiten zu entwickeln, einen richtigen Ansatz.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag daher, Anreize zu schaffen, die Verfallsdatentechnik und andere technische Maßnahmen zum Schutz der Privatsphäre (etwa so genannte Sticky Policies)[303] möglichst intensiv weiterzuentwickeln. Je stärker bereits die technische Infrastruktur datenschutzrechtliche Aspekte berücksichtigt, desto leichter wird es Nutzerinnen und Nutzern fallen, ihre Rechte aktiv wahrzunehmen.

3.8 Selbstdatenschutz und Medienkompetenz

Die Enquete-Kommission hält die Ausbildung und kontinuierliche Förderung von Kompetenz und Eigenverantwortung der Nutzerinnen und Nutzer digitaler Medien und dem damit verbundenen Umgang mit eigenen und fremden personenbezogenen Daten für unverzichtbar. Sie geht davon aus, dass die Nutzung zukünftiger (mobiler) Internetdienste die Entwicklung hin zu einem nutzerorientierten Datenschutzmanagement noch weiter verstärken wird. (Selbst-)Datenschutz, Datenschutzmanagement und IT-Sicherheit müssen deshalb kontinuierlich thematisiert und gestärkt werden. Bildungsangebote müssen für alle Altersstufen entwickelt und zur Verfügung gestellt werden.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag deshalb darauf hinzuwirken, dass die bisherigen Akteure wie beispielsweise die Daten- und Verbraucherschutzverbände sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zusammen mit der geplanten Stiftung Datenschutz noch stärker als bisher zur Förderung von Selbstdatenschutz und Medienkompetenz beitragen. Die Enquete-Kommission betont, dass über die finanzielle Ausstattung der Landesbeauftragten für den Datenschutz allein die Länder entscheiden, unterstützt aber eine Fortführung des Engagements in diesem Bereich.

Hinsichtlich weiterer Handlungsempfehlungen wird auf den Zwischenbericht der Enquete-Kommission zum Thema Medienkompetenz[304] und die Handlungsempfehlungen zur Stiftung Datenschutz[305] verwiesen.

---

[302] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben folgendes ergänzendes Sondervotum zum Kapitel 3.6 *Privacy by Design und Privacy by Default* abgegeben:
„Über die gemeinsam beschlossenen Handlungsempfehlungen hinaus wird dem Deutschen Bundestag empfohlen, die Anbieter von Diensten und Anwendungen, die auf der Erhebung, Verarbeitung und Speicherung personenbezogener Daten basieren beziehungsweise die zu ihrer Funktionserfüllung personenbezogene Daten erheben, verarbeiten und speichern, zu verpflichten, grundsätzlich die höchstmöglichen Datenschutzeinstellungen voreinzustellen (Privacy by Default).“

[303] Mit Sticky Policies wird eine Art von digitalem Rechtemanagement für Daten bezeichnet: Durch angeheftete Metadaten werden zugelassene Verwendungszwecke definiert. Mit „sticky“ ist gemeint, dass diese Metadaten bei Kopiervorgängen „haften bleiben“, also mit übertragen werden: Siehe hierzu auch: Sirix AG security technologies im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik. Ergänzende und alternative Techniken zu Trusted Computing (TC-Erg./-A.), Teil 1. Version vom 29. Januar 2010. S. 20 f. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/TC_ErgA/TC-ErgA_Teil1.pdf

[304] Bundestagsdrucksache 17/7286, online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Medienkompetenz_1707286.pdf

[305] Siehe unten Kapitel 3.21.

3.9 Soziale Netzwerke

Aus datenschutzrechtlicher Sicht werfen soziale Netzwerke eine Reihe von spezifischen Fragestellungen auf. Diese können in Abhängigkeit von den konkreten Produkten der jeweiligen Netzwerkanbieter variieren. Von grundlegender Bedeutung für die Bewertung ist eine klare Trennung zwischen einerseits der Datenverarbeitung durch die Anbieter der Netzwerke selbst und andererseits der Datenverarbeitung durch die Nutzerinnen und Nutzer der Plattformen. Die Enquete-Kommission regt daher an, bestehende Vollzugsdefizite schnellstmöglich zu beseitigen, und empfiehlt zugleich dem Deutschen Bundestag, den Datenschutz bei sozialen Netzwerken in geeigneter Weise zu verbessern.

Für soziale Netzwerke sollten datenschutzfreundliche Grundeinstellungen (Privacy by Default) gesetzlich vorgeschrieben sein. Diese sollten auch die Funktionalität beinhalten, dass in sozialen Netzwerken abgelegte Profile in externen Suchmaschinen nur nach ausdrücklicher Zustimmung des Nutzers auffindbar werden. Zudem müssen die Nutzerinnen und Nutzer eines sozialen Netzwerks jederzeit ihren Account einfach und nachhaltig elektronisch löschen können, das heißt es muss auch zu einer Löschung der Daten auf dem Server des Anbieters kommen. Die Weitergabe von personenbezogenen Daten durch die Betreiber sozialer Netzwerke an Dritte darf neben gegebenenfalls geltenden gesetzlichen Erlaubnistatbeständen nur nach ausdrücklicher Einwilligung durch den Nutzer zulässig sein.[306]

3.10 Datenschutzaufsicht

Die bestehenden Regelungen zur Datenschutzaufsicht sollten aus Sicht der Enquete-Kommission dahingehend überprüft werden, ob sie auch bei den neuen Organisationsformen und vernetzten Prozessen (zum Beispiel Cloud-Computing, Auftragsdatenverarbeitung im Konzern, internationale Diensteanbieter im Internet) einen effektiven Datenschutz sicherstellen. Die Anordnungsbefugnisse des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sollten an dessen Aufsichtsbefugnisse angepasst werden.

Darüber hinaus hat das Urteil des Europäischen Gerichtshofes vom 9. März 2010 zur Unabhängigkeit der deutschen Datenschutzbehörden im nicht-öffentlichen Bereich[307] noch einmal die besondere Rolle der Kontroll- beziehungsweise Aufsichtsbehörden für den Datenschutz hervorgehoben. Aus Sicht der Enquete-Kommission ist es daher unabdingbar, dass die Kontroll- und Aufsichtsbehörden über ausreichende finanzielle, personelle und technische Mittel verfügen, um die ihnen übertragenen Aufgaben effizient und angemessen zu erfüllen. Denn es ist wichtig, dass die Kontroll- und Aufsichtsbehörden die vorhandenen gesetzlichen Befugnisse intensiv ausüben können, damit die bestehenden Datenschutzgesetze effektiv durchgesetzt und Rechtssicherheit geschaffen werden kann.

Die Enquete-Kommission regt darüber hinaus an, dass die Entscheidungen des Düsseldorfer Kreises[308] sowie Einzelpositionen der dort vertretenen Kontroll- und Aufsichtsbehörden zukünftig grundsätzlich veröffentlicht werden und nur in begrenzten Ausnahmefällen eine Veröffentlichung unterbleibt. Auch wenn die Entscheidungen des Düsseldorfer Kreises formal keine unmittelbaren normativen Wirkungen entfalten können, können sie für betroffene Unternehmen zumindest grundlegende Anhaltspunkte bei bestehenden Rechtsunsicherheiten bieten.[309]

3.11 Vorbildwirkung öffentlicher IT-Projekte

Die Enquete-Kommission weist darauf hin, dass sowohl bei der Planung von öffentlichen IT-Projekten und E-Government-Angeboten als auch bei der späteren Aus- und Durchführung die aktuellen technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz in besonderer Weise beachtet und bei technischen Weiterentwicklungen auch fortgeschrieben werden müssen. Nur so können aufkommende Zweifel am sicheren Umgang mit personenbezogenen Daten von Beginn an ausgeräumt werden. Öffentliche IT-Projekte sollten mit Blick auf ihre Vorbildwirkung etwa für die Privatwirtschaft auf hohem Datenschutzniveau durchgeführt werden.

In den letzten Jahren haben verschiedene IT-Großprojekte zum Teil Kritik von Datenschützern erfahren. Die Enquete-Kommission empfiehlt daher,

1. dass öffentliche IT-Projekte auf hohem Schutzniveau basieren und ihrer Vorbildwirkung gerecht werden,
2. dass E-Government-Angebote im Bereich der Dienstleistungen für Bürgerinnen und Bürger den aktuellsten technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz genügen müssen.

Darüber hinaus empfiehlt die Enquete-Kommission bei zentralen IT-Projekten, auch bei jenen, die von der EU eingeleitet werden,

1. den Datenschutz bereits von Beginn an in der Konzeption zu berücksichtigen. Wo dies nicht der Fall ist, muss es auch weiterhin möglich sein, die Umsetzung entsprechender Projekte zu verweigern. Wenn Aufträge für die Entwicklung solcher Projekte vergeben werden, sollten sie stets die Programmierung entsprechender technischer Begrenzungen beinhalten. Im Interesse der Verwirklichung möglichst vorbildlichen Datenschutzes sollte dies bereits bei der finanziellen Planung berücksichtigt werden,

[306] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel 3.9 *Soziale Netzwerke* abgegeben (siehe Kapitel 4.2.2.3).

[307] EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland; siehe auch Kapitel 1.2.3.

[308] Vgl. Kapitel 1.3.6 und 2.3.13.

[309] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel 3.10 *Datenschutzaufsicht* abgegeben (siehe Kapitel 4.2.2.4).

2. den besonderen datenschutzrechtlichen Herausforderungen eines verwaltungsübergreifenden Arbeitens zu begegnen. Um national wie international bei Outsourcing einen unsensiblen Umgang mit Datenschutzbelangen frühzeitig zu verhindern, bedarf es hier einer stärkeren aktiven Einbeziehung datenschutzrechtlicher Aspekte in alle Planungsetappen.

Zudem empfiehlt die Enquete-Kommission dem Deutschen Bundestag, die Forschung im Bereich des Datenschutzes auch weiterhin mit öffentlichen Mitteln zu fördern und zusätzliche finanzielle Anstrengungen zu prüfen, um die Entwicklung von Datenschutztechnologien zu fördern.[310]

3.12 Smartgrids und andere intelligente Netze

Die Möglichkeit, mithilfe intelligenter Stromzähler den tatsächlichen Stromverbrauch kontrollieren zu können, kann einen ökonomischen Mehrwert für die Verbraucher schaffen und beträchtliche ökologische Vorteile mit sich bringen. Bei ihrem Betrieb fallen jedoch auch umfangreiche und differenzierte Datenbestände (Lastprofile) an, die durch geeignete technische und organisatorische Maßnahmen wirksam vor dem Zugriff durch Unberechtigte geschützt werden müssen. Auch muss sichergestellt werden, dass die Datenhoheit, insbesondere ausreichende Kontrollmöglichkeiten, grundsätzlich bei den Verbrauchern verbleiben und diese selbst darüber entscheiden können, wem sie welche Daten zur Verfügung stellen möchten. Dabei muss angesichts der zunehmenden Bedeutung regenerativer Energien bei der Stromversorgung ein effektives Netzmanagement möglich sein.

Es muss sichergestellt werden, dass personenbezogene Daten in der Regel nur den Verbrauchern zur Verfügung gestellt und Verbrauchswerte nur für die Abrechnung personenbezogen verwendet werden dürfen. Darüber hinaus sollten bei ihrer Verwendung zu Zwecken eines verbesserten Netzmanagements Verschlüsselungstechniken zur Anwendung kommen, die eine datenschutzkonforme Datenübermittlung ermöglichen. Zudem müssen ausreichende Sicherheitsvorkehrungen vorgehalten werden, die einen unerlaubten Zugriff auf die Daten verhindern.

Nicht nur im Energiesektor werden derzeit intelligente Netze aufgebaut, zu deren Betrieb umfassend Daten kommuniziert werden müssen. Auch im Verkehrssektor (Verkehrstelematik und E-Mobility), im Gesundheitswesen (Gesundheitstelematik und E-Health) und dem Bildungswesen (E-Learning) befinden sich intelligente Netze in Planung. In diesen Netzen sollen künftig Daten über das eigene Mobilitätsverhalten bis hin zu sensiblen Daten wie dem persönlichen Gesundheitszustand und der Gesundheitshistorie kommuniziert werden.

Datensparsamkeit und Datenvermeidung im Rahmen der für die Nutzung von Zukunftstechnologien erforderlichen Datenverarbeitung sollten Ausgangspunkt entsprechender gesetzgeberischer Initiativen sein. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, in diesen Bereichen die Notwendigkeit gesetzlicher Vorgaben eingehend zu prüfen und darauf hinzuwirken, dass neue Technologien auch bei intelligenten Netzen datenschutzkonform ausgestaltet werden. Einzelfallgesetze für bestimmte Dienste sind dabei nach Möglichkeit zu vermeiden.

3.13 Grundprinzipien des Datenschutzrechts

Die verschiedenen Grundprinzipien des deutschen Datenschutzrechts sind durch die Enquete-Kommission im Kapitel 2.1 ausführlich dargestellt worden. Die Enquete-Kommission geht davon aus, dass trotz rasanter technischer Weiterentwicklungen diese Grundprinzipien auch in Zukunft einen Anspruch auf Geltung haben müssen. Dabei sollten die Grundsätze der Verhältnismäßigkeit, der Datensicherheit und -sparsamkeit, der Zweckbindung und Transparenz noch stärker zur Geltung gebracht werden.

Es muss jedoch auch Anspruch des nationalen Gesetzgebers sein, das Datenschutzrecht unter Berücksichtigung der europarechtlichen Vorgaben fortlaufend weiterzuentwickeln. Vorrang sollte hierbei eine technikneutrale Ausgestaltung von datenschutzrechtlichen Bestimmungen haben. Angesichts einer zunehmenden Komplexität und Länge der Regelungen müssen auch Übersichtlichkeit, Lesbarkeit und die Verständlichkeit eine größere Rolle einnehmen.

Neben sprachlichen Vereinfachungen und Verbesserungen sollten auch aktuelle und zukünftige Entwicklungen bei den Definitionen und Begriffsbestimmungen (beispielsweise zur Personenbeziehbarkeit) durch den Deutschen Bundestag beobachtet werden.

3.14 Auskunfts- und Widerrufsrechte

Bereits nach dem geltenden Datenschutzrecht ist die Wirtschaft gefordert, für Transparenz beim Umgang mit personenbezogenen Daten zu sorgen und den Nutzer nicht im Unklaren über die Speicherung und Nutzung seiner Daten zu lassen. Für die Zukunft empfiehlt die Enquete-Kommission dem Deutschen Bundestag, den Transparenzgrundsatz technikneutral auszugestalten. Für die Nutzerinnen und Nutzer muss insbesondere erkennbar sein, von welcher verantwortlichen Stelle personenbezogene Daten erhoben werden. Wenn Daten weitergegeben oder von anderen genutzt werden, soll unter Berücksichtigung der technisch vorhandenen Möglichkeiten und unter Wahrung des Betriebs- und Geschäftsgeheimnisses eine Rückverfolgbarkeit für den Betroffenen geschaffen werden. Dies könnte die Geltendmachung der Rechte auf Auskunft, Löschung, Sperrung oder Widerspruch weiter erleichtern.

Die Enquete-Kommission empfiehlt zudem eine Befassung des Deutschen Bundestages mit der Frage der Ausübung und weiteren Stärkung von Betroffenenrechten im Bundesdatenschutzgesetz (vergleiche §§ 33 ff. BDSG), insbesondere ob verantwortliche Stellen zu einer besseren

[310] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständige Annette Mühlberg haben ein ergänzendes Sondervotum zum Kapitel 3.11 *Vorbildwirkung öffentlicher IT-Projekte abgegeben* (siehe Kapitel 4.2.2.5).

und verständlicheren Information der Betroffenen über die Verwendung der Daten bei der Erhebung verpflichtet werden können und ob eine effektivere Ausgestaltung der bereits vorhandenen Rechte auf Auskunft, Löschung, Sperrung oder Widerspruch (vergleiche § 4 Absatz 2 und 4 BDSG) denkbar ist. Dabei sollte dem Einsatz moderner Technologien (etwa dem Recht auf elektronische Auskunft über die gespeicherten Daten und einem elektronischen Widerspruchsrecht) besondere Bedeutung zukommen. Denn die Geltendmachung der Betroffenenrechte sollte auf die gleiche Art möglich sein, wie in die Datenerhebung eingewilligt wurde, bei Angeboten im Internet konsequenterweise auch elektronisch.

3.15 Datenbrief

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, ein Datenbrief-Konzept nicht weiter in Erwägung zu ziehen. Der Datenbrief entspräche nicht dem Grundsatz der Datensparsamkeit (vergleiche § 3a BDSG). Für die Zustellung des Datenbriefes wären zumindest die Adresse des betroffenen Nutzers oder andere Kontaktdaten erforderlich, die für den eigentlich in Anspruch genommenen Dienst eventuell gar nicht anfallen würden. Die Daten des Betroffenen müssten möglicherweise zentral – mit erhöhtem Aufwand für die Datensicherheit – in einer Datenbank geführt und laufend aktualisiert werden. Es besteht das Risiko, dass selbst sensible Daten der Betroffenen an unberechtigte Dritte gelangen. Der bürokratische Aufwand aller Beteiligten steht in keinem Verhältnis zum erwarteten Nutzen.

3.16 Anonyme Bezahlsysteme

Mit dem technischen Fortschritt nimmt auch der elektronische Zahlungsverkehr im Internet zu. Zunehmend werden alltägliche Einkäufe im Internet abgewickelt. Hierbei fallen auch eine Vielzahl personenbezogener Daten an. Die Einführung eines digitalen Bargeldes könnte jedoch zu einer Reduzierung der personenbezogenen Daten im Zahlungsverkehr des Internets führen. Darüber hinaus würde eine Einführung des digitalen Bargelds eine Annäherung an alltägliche Barzahlungsgeschäfte in der „realen Welt“ fördern. Sie bietet allerdings auch Risiken, da ein weitestgehend anonymer Zahlungsverkehr zugleich eine Erleichterung für die Begehung von Straftaten sein könnte und damit das Internet als Tatmittel missbraucht würde. Internationale Lösungen sollten daher dann unterstützt werden, wenn sie Chancen und Risiken eines solchen Bezahlungssystems in einen angemessenen Ausgleich setzen. Die Enquete-Kommission regt daher gegenüber der Bundesregierung an, entsprechende Forschungsvorhaben, die sich mit der Einführung eines digitalen Bargelds auseinandersetzen, positiv zu begleiten.

3.17 Technischer Datenschutz

Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme im öffentlichen und nicht-öffentlichen Bereich gegen unberechtigten Zugriff und missbräuchliche Nutzung von innen und außen geschützt sind. Die hierfür einschlägigen Schutzregelungen (zum Beispiel die Anlage zu § 9 BDSG) stammen aus einer Zeit, als Datenverarbeitung durch Großrechner in abgeschotteten Rechenzentren gekennzeichnet war.

Beispielsweise kommen im Zuge des E-Governments längst Onlineverfahren zum Einsatz, bei denen Bürger selbst auf die IT-Systeme der Verwaltung zugreifen. Durch diese Entwicklung und die fortschreitende Vernetzung der Verwaltungssysteme untereinander wird es zunehmend schwieriger, das Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden. Die Enquete-Kommission hält es für erforderlich zu prüfen, ob die technisch-organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes (Anlage zu § 9 BDSG und entsprechende Regelungen in den Datenschutzgesetzen der Länder) durch technikneutrale Schutzziele ersetzt werden müssen, die dann durch dokumentierte Rahmen- und Verfahrenskonzepte umgesetzt und dem aktuellen Stand der Technik entsprechend fortgeschrieben werden müssten.

3.18 Datenschutz für Kinder und Jugendliche

Aktuelle Studien zeigen, dass viele Kinder und Jugendliche mit der Nutzung moderner Technik bereits sicher und selbstverständlich umgehen können. Dennoch hält die Enquete-Kommission auch für die Zukunft ein verstärktes Bemühen um Aufklärung und Bildung im Bereich des Datenschutzes für geboten. Vielversprechende Bildungsangebote staatlicher sowie nicht staatlicher Organisationen liegen hierzu bereits vor. Es gilt daher, diese Angebote noch sichtbarer für die Nutzerinnen und Nutzer zu machen. Die Enquete-Kommission sieht bei der Stärkung des Selbstdatenschutzes von Kindern und Jugendlichen auch die Länder aufgrund ihrer Zuständigkeit für den Bildungsbereich in der Pflicht.

Unternehmen, die Dienste im Internet anbieten, können die Einwilligungsfähigkeit von Minderjährigen bisher nur schwer feststellen. Die Enquete-Kommission empfiehlt daher der Bundesregierung, die gesetzlichen Voraussetzungen der Einwilligungsfähigkeit von Minderjährigen zu überprüfen. In die vorzunehmende Prüfung sollte die bisher maßgebliche Einsichtsfähigkeit, aber auch die Möglichkeit einer festen Altersgrenze einbezogen werden. Dabei ist zu beachten, dass die Informations- und Kommunikationsrechte von Minderjährigen auch in Zukunft gewahrt bleiben.

3.19 Profilbildung

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag zu prüfen, ob die Bildung bestimmter personenbezogener Profile gesetzlich zu regeln ist. Dabei könnten bestimmte Profilbildungen von einer ausdrücklichen gesetzlichen Regelung oder aber der Einwilligung der Betroffenen abhängig gemacht werden.

Insbesondere durch Berechnungen, Vergleiche und statistische Korrelationssoftware können in bestimmten Fällen personenbezogene Daten, die Unternehmen im Rahmen von Internetdiensten erhoben haben, zu umfassenden Pro-

filen zusammengeführt und zu vielfältigen Zwecken genutzt werden. Durch solche Profile können in einigen Bereichen Verhalten, Gewohnheiten und Neigungen eines Nutzers abgebildet und kategorisiert werden, ohne dass es diesem zuvor offengelegt wird.

Für bestimmte Profilbildungen sind daher eine gesetzliche Definition dieses Begriffs sowie Regelungen zum Umgang mit ihnen zu erwägen. Dabei ist zu berücksichtigen, dass nicht jede Verknüpfung von Informationen mit einer natürlichen Person zu einem schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht führt und eine gesetzliche Regelung erfordert. Wichtig ist daher, für diese Fälle eine klare Unterscheidung zu treffen. Transparenz für Betroffene und Informationen über Umfang sowie Herkunft der Profildaten und die beabsichtigte Verwendung des Profils sind notwendig. Diese Ziele könnten auch mit Hilfe von Selbstverpflichtungen erreicht werden.

3.20 Veröffentlichung von Daten im Internet

Bei der Veröffentlichung von personenbezogenen Daten im Internet sind in der Regel immer mehrere Grundrechte in einen angemessenen Ausgleich zu bringen. Neben dem Grundrecht auf informationelle Selbstbestimmung sind dies beispielsweise auch das Grundrecht auf Meinungsfreiheit und das Grundrecht auf Informationsfreiheit. Aber auch die Freiheit der Berichterstattung und das Informationsinteresse der Allgemeinheit können zu berücksichtigen sein. Gesetzliche Regelungen für diesen Bereich können mithin nur eine Konkretisierung verfassungsrechtlicher Grenzen darstellen. Die Enquete-Kommission empfiehlt daher der Bundesregierung, diesen Bereich weiterhin sorgfältig zu beobachten und den Schutz vor schwerwiegenden Eingriffen in das Persönlichkeitsrecht sicherzustellen.

Widerspruchsrechte gegen bestimmte Veröffentlichungen im Internet, die vorrangig auf der Basis von Selbstverpflichtungen von Plattformbetreibern umgesetzt werden könnten, können ein wirksames Mittel zur Wahrung des Grundrechts auf informationelle Selbstbestimmung sein. Allerdings muss es auch hierbei zu einer angemessenen Berücksichtigung verschiedener, möglicherweise auch gegenläufiger, Interessen kommen. Dies muss durch entsprechende verfahrensrechtliche Regelungen abgesichert sein. Bereits bestehende Widerspruchsregelungen (vergleiche § 35 Absatz 5 BDSG, Artikel 14 DSRL) sind mit einzubeziehen.

3.21 Stiftung Datenschutz

Die Enquete-Kommission ist der Ansicht, dass die Errichtung einer Stiftung Datenschutz mit dem Auftrag, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, ein Datenschutzaudit zu entwickeln und Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung verbessern kann. Sie begrüßt daher im Grundsatz die von der Bundesregierung geplante Stiftung Datenschutz.

Diese Stiftung kann unter anderem Kriterien für die Zertifizierung von Diensten sowie für ein einheitliches Gütesiegel aufstellen und damit eine leicht nachzuvollziehende Vergleichbarkeit für Unternehmen und Bürger herstellen. Dadurch kann sich auch eine Erleichterung bei der Auswahl zwischen einer Vielzahl von Anbietern ergeben und zugleich das Vertrauen der Bürger in neue Technologien gestärkt werden. Für Unternehmen kann sie Anreize setzen, hohe datenschutzrechtliche Anforderungen einzuhalten.

Weitere Aufgaben können die Stärkung des Selbstdatenschutzes sowie Aufklärung und Bildung im Datenschutz sein.

Die Enquete-Kommission fordert daher die Bundesregierung bei Errichtung der Stiftung auf, folgende Punkte – die für eine wirkungsvolle Arbeit einer Stiftung Datenschutz mit vorstehendem Auftrag von großer Bedeutung sind – zu berücksichtigen:

1. Die Stiftung ist mit Distanz zu den zu bewertenden Unternehmen zu organisieren. Personell ist darauf zu achten, dass bei der Besetzung der Gremien Unternehmen oder Verbände zwar beteiligt werden, aber auf die Unabhängigkeit der Stiftung an sich keinen Einfluss haben. Dies könnte zum Beispiel durch die Beteiligung in einem Beirat, der beratende Funktion hat, geschehen. Finanziell sollte die Stiftung nicht allein vom Bundeshaushalt abhängig sein. Bei der Annahme von Zuwendungen hat die Stiftung jedoch darauf zu achten, dass ihre Unabhängigkeit nicht gefährdet werden darf.

2. Bei der Entwicklung von Gütesiegeln durch die Stiftung ist darauf zu achten, dass ein einheitliches Gütesiegel geschaffen und somit eine inflationäre Handhabung bei der Vergabe vermieden wird. Ebenso ist das Verfahren für die Vergabe transparent zu gestalten. Die Gütesiegel sind nur für eine bestimmte Zeit zu erteilen und müssen überprüfbar sein.

3. Im Bereich der Bildung sollte die Stiftung Datenschutz sowohl schulisch als auch außerschulisch tätig sein. Sofern sie im schulischen Bereich tätig wird, sollten durch eine Abstimmung mit den Ländern von Beginn an Zuständigkeitsverletzungen ausgeschlossen werden.

4. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Informationsportal oder ein virtuelles Datenschutzbüro zu schaffen. Die Stiftung sollte hier auch eine koordinierende Funktion hinsichtlich entsprechender bereits bestehender Bildungsinitiativen übernehmen.

5. Im Bereich der Datenschutzforschung wird angeregt zu prüfen, ob die Stiftung Datenschutz insbesondere bei der Entwicklung und dem Ausbau von Instrumenten des technischen Datenschutzes tätig werden kann. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der Koordination der Forschungsmittelver-

gabe als auch für den Bereich eigener Forschungsanstrengungen.[311] [312] [313]

4 Sondervoten

Bei den Sondervoten handelt es sich um Textvorschläge, die in der Enquete-Kommission nicht die erforderliche Mehrheit gefunden haben. Sondervoten sind daher nicht Teil des von der Enquete-Kommission beschlossenen Textes. Sofern Sondervoten auch von weiteren Fraktionen oder Sachverständigen befürwortet werden, ist dies durch eine Fußnote an dem entsprechenden Sondervotum kenntlich gemacht.

4.1 Sondervoten zu Kapitel 2

4.1.1 Sondervoten zu Kapitel 2.1

4.1.1.1 Sondervotum der Fraktion BÜNDNIS 90/DIE GRÜNEN zu 2.1.1 *Schutzgegenstand*[314]

Allerdings ist diese Erkenntnis nicht so neu. Daten und Informationen können je nach Kontext, in dem sie relevant werden, personenbeziehbar werden. Deshalb hat der Gesetzgeber im Bundesdatenschutzgesetz mit einem weit auszulegenden Begriff des Personenbezuges reagiert, um sicherzustellen, dass jedenfalls Daten nicht von vornherein aus dem Schutz herausfallen dürfen. Gerade weil erst der jeweilige Verwendungskontext entscheidet, kann es, wie das Bundesverfassungsgericht hervorgehoben hat, keine per se trivialen, nicht schutzwürdigen Daten geben.

Im Hinblick auf einen noch vorgelagerten gefährdungsabhängigen Schutz ist es allerdings notwendig, die Dogmatik des Personenbezugs dynamisch weiterzuentwickeln. So zeigt das Beispiel der Geodaten, aber auch der Scoring-Diskussion, dass die gezielte Verarbeitung von Daten schon vor ihrer Zusammenführung hinsichtlich einer bestimmten Person Risiken dann birgt, wenn sie letztlich darauf abzielt, Einzelne statistisch einzuteilen, und damit erhebliche Benachteiligungen für Personen oder Personengruppen nach sich ziehen kann, wie dies zum Beispiel beim Wohnort-Scoring der Fall ist.

4.1.1.2 Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.1.2 *Erlaubnisvorbehalt*

Überall dort, wo gestörte Vertragsparität vorliegt, sollte die Einwilligung der Betroffenen unwirksam sein, so insbesondere im Abhängigkeitsverhältnis des Arbeitnehmers beziehungsweise des Bewerbers zum Arbeitgeber sowie des Bürgers – beispielsweise als Leistungsempfänger – zum Staat, sofern es für die Abfrage dieser persönlichen Daten keine gesetzliche Grundlage gibt. Auch bei Verträgen zwischen Verbrauchern und Unternehmen existiert keine Parität. So kann zum Beispiel bei Verträgen zu internetbasierten Diensten, die ohne die Einwilligung zur Preisgabe persönlicher Daten, die für die Erbringung des Dienstes selbst nicht benötigt werden, nicht abgeschlossen werden können, von einer freiwilligen Einwilligung nicht ausgegangen werden, wenn diese Dienstleistung nicht auch ohne Datenerhebung erhältlich ist.

4.1.1.3 Ergänzendes Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.1.2 *Erlaubnisvorbehalt*[315]

Die Frage der Freiwilligkeit einer Einwilligung hat in der digitalen Welt an Brisanz gewonnen. Wenn beispielsweise die Nutzung eines Onlinedienstes voraussetzt, dass die Nutzerinnen und Nutzer durch Ankreuzen einer Checkbox der Erhebung ihrer Daten zustimmen, so sind sich die Betroffenen über die Tragweite ihrer Entscheidung häufig nicht im Klaren.

Da sie die entsprechenden Datenschutzbestimmungen des Anbieters beziehungsweise dessen allgemeine Geschäftsbedingungen, in die erstere bisweilen integriert sind, häufig nicht oder nur oberflächlich zur Kenntnis nehmen, erteilen sie im Zweifel eine Einwilligung, die sie bei genauerer Überlegung nicht erteilt hätten. Um zu klären, ob die für eine informierte und freiwillige Entscheidung wichtigen Informationen tatsächlich in ausreichend transparenter Weise vorgelegen haben, ist es dann jedoch bereits zu spät: Die Daten werden erhoben, und der Betroffene ist sich darüber häufig nicht im Klaren. Folglich kommt es im Nachhinein auch nicht mehr zur Überprüfung der Rechtsgültigkeit der erteilten Einwilligung. Die Erfahrung zeigt, dass die Mehrzahl der Internetnutzerinnen und -nutzer Datenschutzerklärungen ebenso wenig liest wie allgemeine Geschäftsbedingungen und dennoch am elektronischen Geschäftsverkehr teilnimmt. Dies deutet darauf hin, dass die Mehrzahl der auf diesem Wege erteilten Einwilligungen nicht tatsächlich freiwillig erteilt worden sind, woraus zu schließen wäre, dass in zahlreichen Fällen Daten ohne rechtliche Grundlage, mindestens aber unter zweifelhaften Umständen erhoben und gespeichert werden. Man erkennt hier, dass die an sich begrüßenswerte Intention des Gesetzgebers, einen maximalen Schutz der personenbezogenen Daten des Einzelnen zu ermöglichen, im Internetzeitalter nicht mehr verwirklicht wird.

Die Praxis der elektronischen Einwilligung nach § 13 Absatz 2 TMG wird von Diensteanbietern systematisch dazu genutzt, den Datenschutz zu unterlaufen, indem sie sich

[311] Die Fraktionen CDU/CSU und FDP sowie die Sachverständigen Prof. Dr. Hubertus Gersdorf, Prof. Dieter Gorny, Dr. Wolf Osthaus und Dr. Bernhard Rohleder haben ein ergänzendes Sondervotum zum Kapitel 3 *Handlungsempfehlungen* abgegeben (siehe Kapitel 4.2.1.2).

[312] Die Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Constanze Kurz und Annette Mühlberg haben gegen die Textfassung der Kapitel 3.13 bis 3.21 gestimmt und ein Sondervotum abgegeben (siehe Kapitel 4.2.2.6).

[313] Weitere ergänzende Sondervoten zu Kapitel 3 *Handlungsempfehlungen* haben die Fraktion SPD sowie die Sachverständigen Alvar Freude, Lothar Schröder und Dr. Wolfgang Schulz (siehe Kapitel 4.2.3), die Fraktion DIE LINKE. sowie die Sachverständigen Constanze Kurz und Annette Mühlberg (siehe Kapitel 4.2.4) und die Fraktion BÜNDNIS 90/DIE GRÜNEN (siehe Kapitel 4.2.5) abgegeben.

[314] Die Fraktion DIE LINKE. schließt sich diesem Sondervotum an.

[315] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Kapitels 2.1.2 *Erlaubnisvorbehalt* an.

auf diese Weise die Zustimmung zu Datenerhebungen von den Nutzerinnen und Nutzern erteilen lassen, die in aller Regel deren Interesse, die eigene Privatsphäre zu schützen, zuwiderlaufen. Anders gesagt: Das bloße „Abklicken“ einer Einwilligung in die Erhebung und Verwendung personenbezogener Daten zu allerlei Zwecken ist nur formal eine freiwillige Einwilligung. Faktisch werden Bürgerinnen und Bürger auf diese Weise entmündigt. Dahinter steht das Interesse der Anbieter, diese Daten zu monetarisieren. Derartige Geschäftsmodelle laufen den Interessen der Bürgerinnen und Bürger auch dann zuwider, wenn sie eine kostenfreie Nutzung des betreffenden Dienstes allererst ermöglichen, weil sie darauf basieren, die Privatsphäre des Einzelnen dem Primat der wirtschaftlichen Wertschöpfung zu unterwerfen.

Schon heute ist bei vielen Onlinediensten für die Nutzerinnen und Nutzer nicht mehr durchschaubar, wozu ihre Daten genutzt werden und in welcher Weise sie im Rahmen von Datenhandel weiterverbreitet werden.

Um das Datenschutzrecht in einer bürgerfreundlichen Weise weiterzuentwickeln, sind Regelungen zu schaffen, die Nutzerinnen und Nutzern ihre verlorene Souveränität wiedergeben. Ihnen müssen Mittel an die Hand gegeben werden, die es ihnen ermöglichen, die Kontrolle über die Erhebung personenbezogener Daten tatsächlich, nicht nur formal selbst auszuüben. Privacy-by-Default-Modelle sind hierfür geeignete Ansatzpunkte. Denkbar sind auch verbindliche Vorgaben für die Diensteanbieter, die es diesen auferlegen, stets auch eine Alternative zu der Option einer „freiwilligen“ Zustimmung zur umfassenden Erhebung personenbezogener Daten anzubieten. Dies könnte beispielsweise dadurch realisiert werden, dass ein aktives Anklicken verschiedener Berechtigungen zwingend vorgeschrieben wird. Die Betroffenen müssten dann jeweils gesondert in die Erhebung und Verarbeitung personenbezogener Daten zu unterschiedlichen Verwendungszwecken, in den Einsatz unterschiedlicher Webtracking-Techniken und unterschiedlicher Cookies einwilligen. Zu bedenken wäre auch, die Einwilligung unter dem Vorbehalt einer Erneuerung zeitlich zu befristen, sodass nach Ablauf einer gewissen Zeit der Nutzer seine Zustimmung erneut abgeben müsste.

Wo von vornherein eine gestörte Vertragsparität vorliegt, sollte die Einwilligung der Betroffenen auch dann unwirksam sein, wenn sie nach derzeit geltendem Recht freiwillig erteilt wurde, da in Abhängigkeitsverhältnissen grundsätzlich nicht davon auszugehen ist, dass Freiwilligkeit im Sinne der gesetzgeberischen Intention tatsächlich gegeben ist. Wenn etwa Sozialhilfeempfänger gegenüber der Bundesagentur für Arbeit in die Erhebung und Speicherung persönlicher Daten einwilligen, weil sie fürchten, dass diese Einwilligung eine Voraussetzung für den Leistungsbezug darstellen könnte, ist dies ebenso problematisch, wie wenn Arbeitnehmer ihrem Arbeitgeber umfassende personenbezogene Daten zur Verfügung stellen. Der im Bundesdatenschutzgesetz vorgesehene Vorbehalt der freiwilligen Einwilligung in die Erhebung personenbezogener Daten ist deshalb nicht unreflektiert auf das Beschäftigungsverhältnis zu übertragen. Vielmehr ist im Falle gestörter Vertragsparität eine Regelung vorzusehen, die die Rechte der jeweils schwächeren Partei wirksam schützt.

4.1.1.4 Ergänzendes Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.1.2 *Prinzip der Datenvermeidung und Datensparsamkeit*[316]

Das Prinzip der Datenvermeidung und Datensparsamkeit sollte durch klare Normierung gestärkt werden. Die zahlreichen Datenskandale der letzten Zeit haben deutlich gemacht, dass die Umsetzung des datenschutzrechtlichen Erforderlichkeitsgrundsatzes in technische Features nur funktionieren kann, wenn die Aufsichtsbehörden bei Nichtbeachtung der Vorschrift wirksame Sanktionen verhängen können. Ziel muss es sein, nur die für einen bestimmten Zweck tatsächlich notwendigen Daten sammeln zu dürfen. Dazu ist eine Normierung des Grundsatzes Privacy by Design erforderlich. Es ist Aufgabe des Gesetzgebers, entsprechende Anreize zu schaffen. Vorstellbar ist beispielsweise ein System der abgestuften Erwiderung, bei dem Anbietern, die sich rechtswidrig verhalten, zunächst ein Warnhinweis zugestellt wird, bevor weitere Sanktionen greifen.

4.1.1.5 Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.1.4 *Informationelle Selbstbestimmung und Internet*[317]

Informationelle Selbstbestimmung und Internet

Das Internet prägt den heutigen Alltag und stellt sich oft als Bereicherung oder praktische Hilfe dar. Die Möglichkeiten zur Information, Kommunikation und Interaktion werden durch das Medium beträchtlich erweitert. Dies machte das Internet auch wirtschaftlich erfolgreich.

Viele dieser Chancen und Möglichkeiten gehen allerdings mit der Speicherung, Verarbeitung und Übermittlung zahlreicher auch personenbezogener Daten einher. Technische und wirtschaftliche Voraussetzung für viele Informations- und Kommunikationsdienste sind personenbezogene Daten der Nutzer. Sie stellen die ökonomische Basis der meisten kostenlosen kommerziellen Internetdienste dar. Häufig wurden diese Angebote sogar erst durch die Nutzung der Kundendaten zu anderen Zwecken wirtschaftlich erfolgreich. Neben den Onlinespielen haben vor allem soziale Netzwerke die Bereitschaft der Nutzerinnen und Nutzer zur Herausgabe ihrer personenbezogenen Daten gefördert und gesellschaftsfähig gemacht. Der „Wandel der Privatheit“ ist somit zuerst die Erschließung der Privatheit für kommerzielle Nutzung. Regelmä-

[316] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Kapitels 2.1.2 *Prinzip der Datenvermeidung und Datensparsamkeit* an.

[317] Die Fraktion BÜNDNIS 90/DIE GRÜNEN schließt sich den letzten vier Absätzen dieses Sondervotums an und befürwortet insoweit eine Ergänzung des von der Enquete-Kommission verabschiedeten Textes.

ßig ist solches Datensammeln missbrauchsanfällig, zumal häufig mehr Daten als erforderlich gespeichert werden. Stets besteht die Gefahr, dass Nichtberechtigte Zugang zu sensiblen Daten erlangen.

Durch die zunehmende Vernetzung, die Möglichkeit der Verknüpfung von personenbezogenen Daten (Persönlichkeitsprofile) und die ständige Weiterentwicklung automatischer Datenerfassungssysteme potenziert sich diese Gefahr in einer Welt der „allgegenwärtigen" Datenverarbeitung. Mit der Computerisierung des Alltags geht die Speicherung nahezu jeder Lebensäußerung der Menschen einher. Vom „smarten" Bad bis zur elektronischen Fahrkarte und der Onlinereservierung für das Abendessen wird nahezu das gesamte Leben einzelner Personen zum Gegenstand von Datenverarbeitungen. Diese Entwicklung hat zweifellos auch positive Seiten. Die mit ihr einhergehenden Risiken betreffen jedoch nahezu alle Bereiche der menschlichen Existenz, sämtliche wirtschaftlichen, kulturellen, religiösen, politischen und sozialen Beziehungen. Hier geht es also nicht nur um das Verhältnis des Bürgers zum Staat, sondern auch um das Verhältnis des Bürgers zu anderen Bürgern oder zu privatwirtschaftlichen Unternehmen.

In dieser Situation ist die Gesellschaft verpflichtet, Antworten über die Grenzen der juristischen Rahmenbedingungen hinaus zu finden. Vor einer juristischen Formung muss der technologische Wandel kulturell, wissenschaftlich und damit letztlich ethisch bewertet werden.

Bisher hat sich ein kontextbezogener und gesetzlich zu gewährender Schutzrahmen mit unterschiedlichen Komponenten auf verschiedenen Ebenen herausgebildet. Dies reicht von europäischen Vorgaben über die gesetzlichen Regelungen im Bundesdatenschutzgesetz (wie beispielsweise dem bußgeldbewehrten Koppelungsverbot des § 28 Absatz 3b BDSG), über die Auferlegung entsprechender Transparenz- und Informationspflichten für Betreiber von Diensten im Internet bis zu einer Förderung der Medienkompetenz der Nutzerinnen und Nutzer für einen verantwortungsvollen Umgang mit den eigenen personenbezogenen Daten.

Dieser verfassungsrechtliche Status quo ist zu erhalten und auszubauen, denn er geht von den richtigen Voraussetzungen aus: Die uneingeschränkte Nutzung personenbezogener Daten kann potenziell in einem Maße in die Freiheitsrechte von Bürgerinnen und Bürgern eingreifen, dass deren Nutzung staatlichen Schutz auslösen muss. Neuartige Schutzkonzepte zu entwickeln, die den modernen technischen Entwicklungen gerecht werden und die Selbstbestimmung der Bürgerinnen und Bürger über ihre Daten stärken, ist dabei die größte Herausforderung für eine zukunftsorientierte Datenschutzpolitik.

Insbesondere im Hinblick auf das Koppelungsverbot besteht in der digitalen Welt noch erheblicher Nachbesserungsbedarf. Diese Vorschrift besagt, dass der Abschluss von Verträgen nicht an die Zustimmung zur Datenweitergabe oder Werbezusendung gekoppelt werden darf. Eine solche Einwilligung ist dem Gesetz zufolge unwirksam, wenn für den Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht zumutbar ist.

Gleichwohl verlangen zahlreiche Diensteanbieter ihren Kundinnen und Kunden ab, in die Einwilligung zur Erhebung von weit mehr persönlichen Daten einzuwilligen, als für die Nutzung des betreffenden Angebots nötig wäre. So brauchen etwa Onlinehändler keineswegs zu speichern, welche Angebote sich Besucher ihrer Seite ansehen. Schon gar nicht brauchen sie die entsprechenden Daten an Dritte weiterzugeben. Gleichwohl lassen sich zahlreiche Onlinehändler genau diese Genehmigung „freiwillig" einräumen, wenn der Nutzer zum ersten Mal einen Kauf tätigt. Einige dieser Anbieter haben zweifellos eine marktbeherrschende Stellung, datenschutzfreundliche Alternativen stehen häufig nicht zur Verfügung.

Noch bedenklicher sieht es bei vielen sozialen Netzwerken aus. Dass diese personenbezogene Daten der Nutzer erheben, liegt zunächst in der Natur der Sache – der Wunsch, persönlich identifizierbar zu sein, liegt der Nutzung eines solchen Angebots schließlich zugrunde. Gleichwohl verlangen zahlreiche soziale Netzwerke ihren Kundinnen und Kunden aber auch eine Einwilligung in die Weitergabe solcher Daten an Dritte ab. Stimmt der Kunde den entsprechenden allgemeinen Geschäftsbedingungen nicht zu, kann er in der Regel das Angebot des betreffenden Netzwerks nicht nutzen. Datenschutzfreundliche Alternativen gibt es kaum, zumal Nutzer unterschiedlicher Netzwerke sich aufgrund der hegemonistischen Abschottung dieser Portale gegen die Konkurrenz nur schwer untereinander vernetzen können.

Da manche sozialen Netzwerke zweifelsohne marktbeherrschende Unternehmen sind, kann auch hier nicht davon ausgegangen werden, dass dem Nutzer solchermaßen erzwungene Einwilligungen bei Vertragsabschluss zuzumuten sind. Die Praxis steht also klar im Widerspruch zum geltenden Recht, wird aber derzeit stillschweigend geduldet, weil die Monetarisierung der Privatsphäre der Bürgerinnen und Bürger für viele Internetunternehmen das einzige Geschäftsmodell ist. Privatwirtschaftlichen Interessen wird hier der Vorrang gegenüber Datenschutzbelangen eingeräumt.

4.1.1.6 Ergänzendes Sondervotum der Fraktion DIE LINKE. zu 2.1.6 *Anonymität und Identitätsmanagement im Internet*[318]

Maßnahmen wie die vorerst gescheiterte Vorratsdatenspeicherung, bei der sämtliche Bewegungen und Kontakte der Nutzerinnen und Nutzer automatisch aufgezeichnet und gespeichert werden, stellen unverhältnismäßige Eingriffe in deren Privatsphäre dar und stehen im Widerspruch zu ihrem Recht auf Anonymität. Auch Netzwerkmanagementmaßnahmen, etwa mit Hilfe von Deep Packet Inspection, bei der die von Nutzern gesendeten und empfangenen Inhalte durchleuchtet werden, sind mit einem Recht auf Anonymität nicht vereinbar.

[318] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Absatzes an.

4.1.1.7 Sondervotum der Fraktion DIE LINKE. zu 2.1.6 *Anonymität und Identitätsmanagement im Internet*

Während jedoch im Bundesdatenschutzgesetz für die Erhebung von Daten grundsätzlich eine freiwillige Einwilligung des Betroffenen vorgesehen ist, erlaubt das Telemediengesetz eine Erhebung und Verwendung von Nutzerdaten, „soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen.“

Insofern dies eine Identifikation des Nutzers voraussetzt, ist hier eine anonyme Nutzung nicht möglich. Allerdings dürfen diese Nutzungsdaten ohne Einwilligung nicht zu anderen als zu Abrechnungszwecken verwendet werden. Insbesondere dürfen sie nicht mit Nutzungsprofilen verknüpft werden, welche der Diensteanbieter vorbehaltlich eines Widerspruchs des Nutzers „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien“ auch dann erstellen darf, wenn der Nutzer ein Pseudonym verwendet. Vielmehr ist die Erstellung von Nutzungsprofilen nur unter der Voraussetzung erlaubt, dass diese „nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“

Personenbezogene Daten dürfen nach dem Telemediengesetz nicht ohne Einwilligung der Betroffenen erhoben werden. Auch kann die Erhebung solcher Daten nicht allein mit der Notwendigkeit einer Abrechnung gerechtfertigt werden, da Diensteanbieter verpflichtet sind, „die Nutzung von Telemedien und ihre Bezahlung anonym und unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“ und die Nutzer über diese Möglichkeit zu informieren.

Anonyme Nutzung und die Verwendung von Pseudonymen sind also grundsätzlich durch das Telemediengesetz geschützt. Gleichwohl wird diskutiert, ob angesichts der grundsätzlichen Personenbeziehbarkeit von Nutzungsprofilen, die eine Folge der technischen Entwicklung ist, eine stärkere gesetzliche Normierung der Vorschriften zur Profilbildung nötig ist. Das Bundesdatenschutzgesetz weist in dieser Hinsicht eine Schutzlücke auf.

4.1.1.8 Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.1.8 *Selbstdatenschutz und Medienkompetenz*

Allerdings kann die Förderung eines selbstbestimmten Umgangs mit den eigenen Daten nicht als Alternative zu gesetzlichem Datenschutz begriffen werden. Im Gegenteil, je weniger offensichtlich für den einzelnen Bürger erkennbar ist, dass Daten von ihm erhoben, womöglich gar im Hintergrund verknüpft werden, desto mehr ist der Gesetzgeber in der Pflicht, mit klaren Normierungen dafür zu sorgen, dass das Recht auf informationelle Selbstbestimmung keine Leerformel bleibt. Die Anbieter, die auf elektronischem Wege Daten erheben, um diese zu monetarisieren, haben naturgemäß kein Interesse daran, in transparenter Weise darzustellen, zu welchen Zwecken Daten erhoben und genutzt werden, weil sie dann riskieren würden, dass datenschutzbewusste Nutzerinnen und Nutzer zu konkurrierenden Angeboten wechseln würden.

Das Ziel, es Nutzern zu ermöglichen, möglichst kompetent, informiert und selbstverantwortlich mit ihren Daten umzugehen, steht also in einem direkten Widerspruch zum Geschäftsmodell der meisten Anbieter. Mehr Datenschutz- und Medienkompetenz auf Seiten der Nutzerinnen und Nutzer zu fordern, darf für den Gesetzgeber deshalb nicht die Alternative zu klaren Regelungen sein, durch die die Anbieter einerseits zu Transparenz, andererseits zur Einhaltung geltender datenschutzrechtlicher Bestimmungen gezwungen werden. Auch dürfen Schwierigkeiten bei der Durchsetzung von Datenschutz im internationalen Kontext kein Vorwand dafür sein, auf datenschutzrechtliche Neugestaltung zu verzichten und stattdessen auf die Eigenverantwortlichkeit der Nutzer zu verweisen.

Die Förderung der Kompetenz zum Selbstdatenschutz kann vielmehr stets nur eine Ergänzung zu datenschutzrechtlichen Regeln sein, die den Spielraum jener Unternehmen, deren Geschäftsmodelle auf Datenhandel basieren, auf ein zivilgesellschaftlich verträgliches Maß reduzieren.

4.1.1.9 Sondervotum der Fraktion DIE LINKE. sowie der Sachverständigen Constanze Kurz und Annette Mühlberg zu 2.1.10 *Datenschutz für Kinder und Jugendliche*

Der Datenschutz bei besonders schutzwürdigen Gruppen bedarf besonderer Aufmerksamkeit. Die Ausnutzung der neuen informationstechnischen Möglichkeiten darf nicht zulasten der schwächsten Glieder (etwa Kinder und Heranwachsende) unserer Gesellschaft gehen. Gleichzeitig sollen sie aber auch nicht von einer angemessenen Teilhabe an der Informationsgesellschaft ausgeschlossen sein.

Daten von Kindern werden in einem kaum geringeren Umfang als Daten von Erwachsenen erhoben, verarbeitet und weitergegeben. Eine Vielzahl der Unternehmen unterscheidet hinsichtlich ihrer Internetangebote und der damit verknüpften Datenverarbeitungen nicht oder kaum zwischen Erwachsenen und Kindern bzw. Jugendlichen. Auch Kinder und Jugendliche sind heute selbstverständlich aktive Nutzer von Informationsdiensten und setzen diese zum Informationsaustausch ein. Doch ebenso selbstverständlich sind dabei auch Kinder von Geburt an ebenso wie Erwachsene Träger von Grundrechten. Dazu gehört auch das Grundrecht auf informationelle Selbstbestimmung, so dass auch Kinder und Jugendliche alle Datenschutzrechte und damit grundsätzlich das Recht haben, über die Herausgabe und Verwendung ihrer personenbezogenen Daten selbst zu bestimmen. Sie wachsen bereits mit der Nutzung von digitaler Technik und der Angebotsvielfalt des Internets auf und sind damit die am besten vernetzte Altersgruppe: 98 Prozent der 10- bis 18-Jährigen nutzen mittlerweile das Internet. Dies hat eine Studie im Auftrag des Verbandes BITKOM „Jugend 2.0“ ergeben. Selbst Kinder von 10 bis 12 Jahren sind zu 96 Prozent online. Fast schon selbstverständlich ist für Teenager

die Mitgliedschaft in Internet-Gemeinschaften. Nach der Studie sind 77 Prozent in verschiedenen „Communitys“ angemeldet, 74 Prozent nutzen sie aktiv.

Da bereits drei Viertel aller deutschen Kinder und Jugendlichen in sozialen Netzwerken Mitglied sind und regelmäßig über diese Plattformen kommunizieren, entsteht teilweise bereits von jungen Teenagern ein genaues Persönlichkeitsprofil und ein digitales Abbild ihrer Wünsche, Vorlieben, Beziehungsgeflechte, Gewohnheiten. Bekanntlich beruht das Geschäftsmodell der Social Networks im Wesentlichen darauf, Daten ihrer Nutzer zu erheben und kommerziell zu verwerten. Schon im Hinblick auf Erwachsene erscheint diese Nutzbarmachung von Teilen der Privatsphäre für wirtschaftliche Zwecke bedenklich, erst recht jedoch bei Kindern und Jugendlichen. Letztere verfügen häufig noch nicht über das nötige Reflektionsvermögen, um die Nutzung des Angebots mit dem Geschäftsmodell in Verbindung zu bringen. Sie sind sich oft gar nicht darüber im Klaren, dass sie statt mit Geld mit ihren persönlichen Daten für diese Angebote bezahlen. Erst recht überblicken sie oft nicht die langfristigen Folgen ihren Handelns, können also etwa die Gefahr einer vom Nutzer nicht zu kontrollierenden Profilbildung oder erstellten Prognosen durch die Anbieter noch nicht zutreffend einschätzen und bewerten. Darüber kann auch ein diffuses Unwohlsein und die wachsende Sensibilisierung der Betroffenen im Hinblick auf den Datenschutz nicht hinwegtäuschen. Zwar heißt es in der erwähnten BITKOM-Untersuchung, 58 Prozent aller 10- bis 18-Jährigen wünschten sich mehr Datenschutz. Es wäre jedoch gewagt, hieraus zu folgern, die Betroffenen wären sich der umfassenden Nutzung ihrer Daten zu kommerziellen Zwecken der Anbieter stets bewusst oder gar in der Lage, sich auf der Grundlage solcher Kenntnis aktiv gegen die Nutzung ihrer Daten zu entscheiden.

Was bei den Geschäftsmodellen der Social Networks problematisch ist, ist bei Angeboten, die speziell auf Kinder und Jugendliche zugeschnitten sind, besonders bedenklich. Dies gilt nicht nur für die Auswertung des Nutzungs- und Surfverhaltens, sondern auch für die Werbepraktiken bei solchen Angeboten. So können die Betroffenen häufig Werbung und redaktionelle Inhalte weniger klar auseinanderhalten, als dies Erwachsenen möglich ist. Sie sind für personalisierte Werbung mithin empfänglicher und somit manipulierbarer als andere Nutzer, die über mehr Medienerfahrung verfügen. Insbesondere bemerken Kinder es oft nicht, wenn sie von redaktionell betreuten Seiten auf rein kommerzielle Werbeangebote umgeleitet werden, weil die Trennung redaktioneller Inhalte von Werbeinhalten häufig nicht klar erkennbar ist oder bewusst verschleiert wird. Ein Datenschutzproblem ergibt sich daraus beispielsweise schon dann, wenn in diesem Zusammenhang von Werbetreibenden Cookies gesetzt werden, die eine weitere Auswertung des Surfverhaltens der Nutzer auch jenseits des ursprünglichen Angebots ermöglicht.

Ein weiteres, eng damit verbundenes Problem ist die zunehmende Verschuldung schon von Minderjährigen. Beruhend auf der Analyse ihrer hinterlassenen Daten werden Heranwachsende oft mit auf sie zugeschnittenen, manipulativen Werbebotschaften zu übermäßigem, ihren finanziellen Verhältnissen nicht angemessenen Konsum angeregt.

Als Konsequenz aus den obigen Befunden stellt sich die Frage, ob Kinder und Heranwachsende, die nicht wie Erwachsene langfristige Folgen ihres Handelns abschätzen können, in stärkerem Maße einer öffentlichen Fürsorge und eines gesetzlichen Schutzes bedürfen und ob es in diesem Zusammenhang ermöglicht werden muss, Geschäftsmodelle der Anbieter, die nach dem derzeitigen Datenschutzgesetz noch legal sind, im Interesse des Schutzes von Kindern und Jugendlichen einzuschränken.

4.1.2 Sondervoten zu Kapitel 2.2

4.1.2.1 Ergänzendes Sondervotum der Fraktion DIE LINKE. zu 2.2.1.2 *Das Bundesdatenschutzgesetz (BDSG)*[319]

Wenn durch die Politik allerdings immer weitere Einschränkungen des Datenschutzes zur vorgeblichen Bekämpfung von Kriminalität und zur Terrorismusabwehr vorgenommen werden, sinkt sogleich die Möglichkeit, glaubwürdig Einfluss auf den Umgang von nicht staatlichen Akteuren mit persönlichen Daten zu nehmen. Hier sei exemplarisch auf den sprunghaften Anstieg der Kontoabfragen durch Finanz- und Sozialverwaltungen in den letzten Jahren hingewiesen, die im direkten Zusammenhang mit Erweiterungen bei Banken und Sparkassen stehen. So droht der Vorbildcharakter des Staates im Bereich des Datenschutzes verloren zu gehen.

4.1.2.2 Sondervotum der Fraktion DIE LINKE. zu 2.2.1.4 *Herausforderungen für das Datenschutzrecht in öffentlichen Einrichtungen*

Regelmäßig lassen sich zum Teil deutliche Modifikationen der zulässigen Datenerhebungen erreichen, aber ein grundsätzlicher Verzicht auf „Datensammelprojekte“ wird politisch oftmals nicht erreicht. Stattdessen kam und kommt ein Schutzprogramm des Datenschutzes zur Anwendung, das zu großen Teilen mit der technischen Entwicklung nicht Schritt gehalten hat und deshalb oftmals nicht zu passen scheint. Dementsprechend wird auch im Bereich der öffentlichen Verwaltung von massiven Vollzugsdefiziten hinsichtlich des Datenschutzes gesprochen, obwohl dort eine längere Tradition des Umganges mit diesem Recht sowie eine weitaus selbstverständlichere Bindung an das Gesetz besteht. Auch das Aufsichtssystem des Datenschutzes wirft insoweit Fragen auf, als die fehlende Unabhängigkeit der in Landeszuständigkeit erfolgenden Datenschutzaufsicht vom Europäischen Gerichtshof gerügt wurde, aber bis heute folgenlos geblieben ist. Beim Betrieb bestehender oder der Einführung neuer IT-Infrastrukturen in öffentlichen Einrichtungen er-

[319] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Absatzes an.

geben sich eine Vielzahl datenschutzrechtlicher Fragestellungen.

4.1.3 Sondervoten zu Kapitel 2.3

4.1.3.1 Sondervotum der Fraktion BÜNDNIS 90/DIE GRÜNEN zu 2.3.1.1 *Datenschutz in der Informations- und Kommunikationsgesellschaft: Zum Spannungsverhältnis und Gebot der Abwägung zwischen Persönlichkeitsrechten und Kommunikationsgrundrechten*[320]

Die Besonderheit des Schutzgegenstandes

Weil Information und Kommunikation Grundbedingungen unter anderem der Persönlichkeitsbildung und -darstellung sind, gehen eigentumsanaloge Konzeptionen informationeller Selbstbestimmung fehl. Informationen entstehen aus Daten erst in konkreten Verwendungszusammenhängen, wobei der Konstruktion des Verwenders überragende Bedeutung zukommt. Deshalb sind Vorstellungen eines eigentumsanalogen Informationsbeherrschungsrechts von vornherein schief. Schutzkonstruktionen müssen deshalb stets berücksichtigen, dass sich kommunikative Selbstbestimmung in konkreten gesellschaftlichen Zusammenhängen entfaltet, die Voraussetzung für dessen Geltendmachung sind. Es geht also um ein Recht auf Schaffung und Erhalt der Bedingungen, unter denen eine freiheitliche Darstellung der Persönlichkeit möglich ist. Artikel 2 Absatz 1 GG formuliert damit eine Grundbedingung freier Kommunikationsverfassung. Es geht um die Verpflichtung des Gesetzgebers, den Kommunikationsprozess so abzusichern, dass die kommunikative Selbstbestimmung der Bürgerinnen und Bürger möglich bleibt.

Das Grundrecht schützt dabei vor dem Staat wie anderweitigen sozialen Institutionen gleichermaßen. Die Ebene freiwilliger Preisgabe personenbezogener Informationen durch Grundrechtsträger selbst kann bereits als Ausübung allgemeiner Handlungsfreiheit angesehen werden und betrifft ersichtlich nicht das Schutzprogramm des Rechts auf informationelle Selbstbestimmung. Mit diesem wird die Teilhabe der Einzelnen an kommunikativen Prozessen gesichert. Deshalb müssen Verarbeitungen für Betroffene transparent sein, Gestaltungsrechte eingeräumt werden, aber auch und vor allem die Verwendungszusammenhänge beim Verarbeiter selbst und damit die Bildung der Informationen reguliert werden. Dazu braucht es objektiv-rechtliche Gehalte wie zum Beispiel aufgabenbezogene Erhebungs- und Verarbeitungsregeln.

Entgegenstehende Grundrechte der Datenverarbeiter

Einschränkungen dieser Regelungen zum Schutz informationeller Selbstbestimmung sind nur insoweit zulässig, als sie im überwiegenden Allgemeininteresse liegen.[321]

[320] Die Fraktion DIE LINKE. und die Sachverständige Annette Mühlberg schließen sich diesem Sondervotum an.

[321] BVerfGE 65, 1, 43 f. – Volkszählung.

So kann es zu Einschränkungen der informationellen Selbstbestimmung kommen, wenn Grundrechte miteinander kollidieren. In Betracht kommt etwa für die Phase der Erhebung von Daten das Grundrecht der Informationsfreiheit nach Artikel 5 Absatz 1 Satz 1 GG sowie für die Übermittlung das Grundrecht der Meinungsfreiheit des Artikel 5 Absatz 1 Satz 1 GG. Allerdings enden diese dort, wo das berechtigte Interesse oder das Recht auf informationelle Selbstbestimmung eines anderen beginnt. Insbesondere begründet die Informationsfreiheit keinen Anspruch für das Marketing, sich über das Recht auf informationelle Selbstbestimmung hinwegzusetzen.[322]

Regelungen, die betroffenen Personen die Autonomie über die Eröffnung von Informationsquellen sichern sollen, stellen keinen Eingriff in die Informationsfreiheit dar.[323]

Bei der Meinungsfreiheit ist zu bedenken, dass sie sich auf die individuelle Meinungsbildung und den individuellen Meinungsaustausch beschränkt, nicht alle Phasen und Verarbeitungsformen umfasst und durch allgemeine Gesetze wie die Datenschutzgesetze, die sich nicht auf bestimmte Meinungen beziehen, eingeschränkt werden kann. Gesetzliche Regelungen, die den Auftrag zum Schutz der informationellen Selbstbestimmung risikobezogen umsetzen, sind deshalb auch im Geltungsbereich des Artikel 5 Absatz 1 Satz 1 GG zulässig, wenn sie die besondere Bedeutung der Informations- und Meinungsäußerungsfreiheit berücksichtigen. Artikel 5 Absatz 1 Satz 1 GG ist auch keine „allgemeine Kommunikationsverfassung" zu entnehmen, die personenbezogene Daten pauschal dem Schutz des Grundgesetzes entzieht, nur weil deren Veröffentlichung einem wie auch immer gearteten „Kommunikationsprozess" des Internets dienlich sein kann. Weiter in Betracht kommt die Unternehmerfreiheit, soweit sie als Bestandteil der Freiheit der Berufsausübung anerkannt ist. Doch an diese können regelmäßig Anforderungen gestellt werden, wenn sie vernünftigen Gründen des Allgemeinwohls entsprechen. Gesetzliche Regelungen, die die Datenverarbeitung risikoorientierten Anforderungen unterwerfen, sind daher grundsätzlich mit Artikel 12 Absatz 1 GG vereinbar.[324]

Soweit das Grundrecht auf Eigentum gegen Regelungen zum Schutz personenbezogener Daten angeführt wird, gilt, dass der Schutz des Eigentums sich nur auf das Erworbene, nicht jedoch auf die Tätigkeit des Erwerbens selbst bezieht. Damit verbleiben allenfalls wenige denkbare Fallgestaltungen möglicher Kollisionen. Zum Teil wird die wirtschaftliche Betätigungsfreiheit als Unterfall der allgemeinen Handlungsfreiheit nach Artikel 2 Absatz 1 GG als eigentliche Grundlage des Grundrechtsschutzes der Datenverarbeiter angesehen. Ausgangspunkt

[322] So zum Beispiel Simitis, Spiros: Kommentar zum BDSG. 5. Auflage, § 1 Rn. 91.

[323] So zum Beispiel Schulz, Wolfgang: Verfassungsrechtlicher „Datenschutzauftrag" in der Informationsgesellschaft. Die Verwaltung 1999, 137 (149).

[324] Vgl. nur Schulz, Wolfgang: Verfassungsrechtlicher „Datenschutzauftrag" in der Informationsgesellschaft. Die Verwaltung 1999, 137 (148).

des Gesetzgebers müsse die Freiheit aller Datenverarbeitung, nicht ihre Beschränkung sein. Diese Auffassung, die sich darauf gründet, dass kein manifestierter Geheimhaltungswille vorliege oder gesetzlich anerkannt sei, hat sich nicht durchgesetzt. Stattdessen wurde mit dem Recht auf informationelle Selbstbestimmung ein Entscheidungsvorrang der betroffenen Person über Daten, die sich auf ihre sachlichen und persönlichen Verhältnisse beziehen, geschaffen. Die allgemeine Handlungsfreiheit steht zudem unter dem Vorbehalt der verfassungsmäßigen Ordnung und der Rechte Dritter. Sie endet regelmäßig dort, wo das informationelle Selbstbestimmungsrecht eines anderen beginnt.

Nutzerprofilierung und veröffentlichte Daten

Vor diesem Hintergrund sowie dem Hintergrund der konkreten Regelungen der Datenschutzgesetze sind deshalb die jeweils ganz unterschiedlich gelagerten Problemfälle im Kontext des Internets zu bearbeiten. Im Mittelpunkt stehen dabei immer wieder Fälle der Veröffentlichung von personenbezogenen Daten im Internet. Dabei ist jeweils sorgfältig zu differenzieren, ob etwa Datenverarbeitungen im Verhältnis von kommerziellen Anbietern (zum Beispiel Plattformbetreiber wie etwa soziale Netzwerke; Suchmaschinen) zu betroffenen Bürgerinnen und Bürgern oder etwa im Verhältnis von Bürgerinnen und Bürgern untereinander gemeint sind (so genanntes Web 2.0) und etwa zu welchen Zwecken die Veröffentlichungen mit welchen möglichen Risiken erfolgen. So bietet etwa die so genannte Spickmich-Entscheidung des BGH[325] eine erste Klärung hinsichtlich der Verantwortlichkeit der Betreiber von Bewertungsplattformen selbst im Umgang mit den ihnen anvertrauten personenbezogenen Daten. Im Ergebnis wird das Bundesdatenschutzgesetz für anwendbar erklärt, allerdings angesichts dieser neuen Verarbeitungsform die einschlägige Gesetzesbestimmung verfassungskonform ausgelegt. Der Fall offenbart damit einen konkreten Reformbedarf der Bestimmungen des Bundesdatenschutzgesetzes. Hinsichtlich solcher Intermediäre wie Suchmaschinen oder sozialer Netzwerke liegt die Besonderheit dieser Dienste gerade darin, dass sie einerseits für die Nutzbarkeit des Internets geradezu überragend wichtige Angebote eröffnen, die Information und Kommunikation deutlich erleichtern. Zugleich basiert ihr Erfolg allerdings auf der Verarbeitung aller erhältlichen personenbezogenen Daten, welche zu Marketingzwecken systematisch und umfassend ausgewertet und verwendet werden. Die dabei veröffentlichten personenbezogenen Informationen sind in der Dimension des Internets weltweit und oftmals dauerhaft für jede Nutzerin und jeden Nutzer verfügbar. Hinsichtlich der im Hintergrund sich bildenden Nutzerprofilinformationen entstehen ganz neuartige Informationszusammenhänge zu Einzelpersonen, deren Umfang weitestgehend intransparent bleibt. Zutreffend wird mit Blick auf Dienste des Mitmach-Web wie den sozialen Netzwerken, Blogs etc. konstatiert, dass heute Einzelne nahezu problemlos durch Webveröffentlichungen selbst Massenkommunikation betreiben können. Wenn diese Beiträge eine meinungsbildende Funktion haben, ergeben sich auch hier Grundrechtskollisionen, die besondere Probleme hinsichtlich der Anwendbarkeit und der Durchsetzbarkeit der Datenschutzrechte der Bürgerinnen und Bürger untereinander aufweisen. Hier wird allgemein ein erheblicher Regelungsbedarf konstatiert, der bereits auch zu konkreten Gesetzesvorschlägen geführt hat.

4.1.3.2 Ergänzendes Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.3.4 *Verfallsdaten im Internet, regelmäßig erneuerbare Zustimmungspflicht*[326]

Allerdings ist die Technik einem permanenten Wandel unterworfen. Im Rahmen der Technologieförderung durch das Bundesministerium für Wirtschaft und Technologie könnten beispielsweise gezielt Projekte gefördert werden, welche auf die Entwicklung von Datenschutztechniken abzielen. Da die Erhebung und Speicherung privater Daten für viele Unternehmen mittlerweile einen festen Bestandteil ihres Geschäftsmodells darstellen, hat die private Wirtschaft verständlicherweise bislang kaum ein Interesse an der Entwicklung derartiger Techniken gehabt. So man ein „Recht auf Vergessen" für politisch sinnvoll und wünschenswert hält, hätte die Politik jedoch die Möglichkeit, entsprechende Anreize zu setzen.

Bereits heute gibt es Techniken, die in eine ähnliche Richtung weisen. So ist etwa eine zeitlich begrenzte Ver- und Entschlüsselung von Daten möglich, wenn diese nicht bei dem jeweiligen Anbieter, sondern bei spezialisierten Trust Center abgelegt werden. Daten, die von Nutzern freiwillig zur Verfügung gestellt werden, können also jeweils beim Abruf entschlüsselt werden – so lange, bis eine dafür festgelegte Befristung abläuft. Entscheidend für die technische Funktionalität sind dabei so genannte sticky policies, die festlegen, welche Metadaten zusammen mit den Nutzdaten gespeichert und übertragen werden.

Jenseits der Technik sind zudem gesetzgeberische Initiativen denkbar. So könnten Anbieter dazu verpflichtet werden, freiwillige Einwilligungen der Nutzer grundsätzlich nur befristet einzuholen. Das würde bedeuten, dass Letztere nach Ablauf einer gewissen Frist ihr Einverständnis mit der Datenerhebung durch den Anbieter aktiv erneuern müssten. Insofern Daten ohnehin nur zu klar definierten Zwecken erhoben werden dürfen, stünde eine solche Regelung im Einklang mit der Grundintention des ohnehin schon geltenden Rechts. Ein Zweck, für den Daten unbefristet lange gespeichert werden müssten, ist schlichtweg nicht denkbar.

---

[325] BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich.de.

[326] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Absatzes an.

4.1.3.3 Sondervotum der Fraktion DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.3.9 *Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft*

Die staatliche Aufsicht über die Einhaltung datenschutzrechtlicher Bestimmungen stößt im Zuge neuer technischer Entwicklungen immer mehr an Grenzen. Dies kann als Folge einer mangelnden personellen Ausstattung der zuständigen Behörden betrachtet werden, ist jedoch sicher auch der Schwierigkeit geschuldet, in einer zunehmend vernetzten Welt eine effektive Kontrolle auszuüben. Je mehr Daten erhoben, gespeichert und kopiert werden, desto schwerer ist ihre Verbreitung nachzuvollziehen. Folglich sind die Behörden bei der Durchsetzung des Datenschutzrechts stets auch auf die Mitarbeit der privaten Unternehmen angewiesen.

In letzter Zeit wird daraus oft der Schluss gezogen, die Defizite staatlicher Aufsicht könnten durch eine stärkere Einbindung der Unternehmen in die Festsetzung und Durchsetzung von Datenschutzstandards ausgeglichen werden. Selbstverpflichtungen der Internetwirtschaft werden immer häufiger als Alternative zu möglicherweise rigiden gesetzlichen Vorgaben dargestellt. In Eigeninitiative könne die Wirtschaft kurzfristiger und flexibler auf neue Herausforderungen reagieren. Regulierte Selbstregulierung heißt dabei das Schlagwort.

Derartige Bestrebungen begegnen allerdings auch skeptischen Einwänden. Denn Selbstregulierung kann nur dann eine Alternative zu gesetzlicher Normierung darstellen, wenn klar definiert ist, in welchen Grenzen sie sich bewegt, wie sie konkret umgesetzt wird, wer für die Umsetzung der Selbstverpflichtung in den Unternehmen verantwortlich ist, welche Sanktionen im Falle einer Nichtumsetzung drohen und unter welchen Umständen der Gesetzgeber sich vorbehält, einen zunächst der Selbstregulierung überlassenen Bereich nachträglich doch noch gesetzlich zu regulieren. Absichtserklärungen und Willensbekundungen privater Unternehmen stellen keine Alternative zu gesetzgeberischem Handeln dar, wenn ihre Nichtumsetzung mit keinerlei Sanktionen behaftet ist. Eine effektive Selbstregulierung zu etablieren, setzt also voraus, dass Kontroll- und Evaluationsmechanismen entwickelt werden, kurz- und langfristige Ziele klar ausformuliert und Sanktionen für den Fall eines Scheiterns der Selbstregulierung vorgesehen sind.

Anders gesagt: Regulierte Selbstregulierung darf nicht als Rückzug des Gesetzgebers zugunsten einer Selbstdisziplinierung der privaten Wirtschaft verstanden werden, sondern kann stets nur eine Ergänzung innerhalb des vom Datenschutzrecht vorgegebenen Rahmens darstellen. Ob zum Beispiel der freiwillige Datenschutzkodex für Geodatendienste diesem Anspruch gerecht wird oder zukünftig gesetzgeberisch ergänzt werden sollte, braucht an dieser Stelle nicht erörtert zu werden. Auch Skeptiker werden jedoch einräumen, dass Initiativen zur Selbstregulierung, wie sie etwa von der EU-Kommission befürwortet werden[327], stets zu begrüßen sind, wenn sie tatsächlich zu mehr Transparenz und Selbstbestimmungsmöglichkeiten für die Nutzer beitragen.

4.1.3.4 Sondervotum der Fraktion BÜNDNIS 90/DIE GRÜNEN zu 2.3.9 *Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft*

Die Grenzen des ordnungsrechtlichen Aufsichtsansatzes haben deshalb bereits in den 1980er Jahren Diskussionen über alternative Steuerungsansätze ausgelöst. Durchgesetzt haben sich auf EU- wie auch auf Bundesebene beispielsweise die Einführung von Betriebsdatenschutzbeauftragten sowie Vorabkontrollen, mit denen die Kontrolle in die Betriebe verlegt wird. Potenzielle Defizite staatlicher Aufsicht können damit durch eine Einbindung der Unternehmen in die Durchsetzung von Datenschutzstandards zumindest teilweise ausgeglichen werden.

4.1.3.5 Sondervotum der Fraktionen DIE LINKE. und der Sachverständigen Annette Mühlberg zu 2.3.12 *Beschäftigtendatenschutz*

Aktuell werden Beschäftigtendaten im Rahmen der allgemeinen Normen, wie Bundesdatenschutzgesetz, Telekommunikationsgesetz, oder im (kollektiven) Arbeitsrecht, wie im Betriebsverfassungsgesetz, geregelt. Im Bundesbeamtengesetz wird der Umgang mit der Personalakte im Beamtenverhältnis geregelt. Andere spezialgesetzliche Normen hinsichtlich des Datenschutzes für private oder öffentliche Arbeitgeber existieren nicht. Die oft darüber hinausgehenden Sachverhalte zum Schutz der Beschäftigtendaten hat der Gesetzgeber der Rechtsprechung in Form einer Vielzahl von Einzelentscheidungen des Bundesarbeits- und des Bundesverfassungsgerichts überlassen.

Datenschutzskandale in der Vergangenheit bei verschiedenen deutschen Großunternehmen haben gezeigt, dass eine Diskrepanz zwischen dem Recht der Beschäftigten auf informationelle Selbstbestimmung und dem Recht des Arbeitgebers auf Schutz des Eigentums in dem besonders zu betrachtenden Arbeitsverhältnis besteht und es hier einer Regelung durch den Gesetzgeber bedarf.

Im Bereich der Beschäftigtendaten gilt es deshalb, das Persönlichkeitsrecht des Beschäftigten einerseits zu schützen, dem Arbeitgeber aber auch Möglichkeiten zu geben, seine Rechte wahrzunehmen. Der Gesetzgeber hat bereits erkannt, dass es hier gesetzlicher Regeln bedarf.

Dies gilt insbesondere in einer Welt des digitalen Wandels mit immer neueren, komplexeren Möglichkeiten der

[327] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4. November 2010, KOM(2010) 609, Kapitel 2.2.5, online abrufbar unter: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf

Datenverarbeitung, die in den Arbeitsalltag hineinwirken. Hier muss der Schutz von Beschäftigtendaten einen bedeutenderen Stellenwert bekommen. Auch das Privatleben unterliegt in den vergangenen Jahren einem rasanten technischen Wandel, der anhält und stetig komplexer wird. Die Benutzung von Internet, E-Mail-Systemen, sozialen Netzwerken, Mobiltelefonen, Onlinebanking, Kreditkarten oder Bonuskartensystemen im Privatleben hat Einfluss auf das Berufsleben, weil im Netz persönliche Daten dokumentiert und Arbeitgebern zugänglich gemacht werden. Es fallen persönliche Daten an, die oft nur unzureichend gegen unrechtmäßige Nutzung und Weitergabe an Dritte gesichert sind.

Im Arbeitsverhältnis werden Chipkarten eingesetzt, die den Zugang der Beschäftigten aufzeichnen, bei der Verwendung von RFID (Radio Frequency Identification) können Tätigkeitsprofile erstellt werden und Handys ermöglichen über GPS jederzeit die Feststellung, wo sich Beschäftigte befinden. Durch vielfältige Spuren im Netz steigen die Möglichkeiten, Leistungsüberprüfungen von Beschäftigten durchzuführen. Hinzu kommt außerdem, dass unter den Stichwort Terrorbekämpfung von staatlichen Stellen über den Arbeitgeber im Rahmen so genannter Sicherheitsüberprüfungen Daten, etwa über religiöse Präferenzen oder ethnische Herkunft weitergegeben werden, obwohl diese Daten dem Persönlichkeitsschutz unterliegen. Außerdem entstehen durch Verfahren wie ELENA (elektronischer Entgeltnachweis) oder die geplante Gesundheitskarte riesige Datenmengen, deren Verwendung zwar gesetzlich geregelt wurde, die aber Anlass für Kritik geben. Diese Auffassung wird auch von Seiten der Landesbeauftragten für den Datenschutz geteilt.

Darüber hinaus bedienen sich Arbeitgeber immer neuerer Techniken (wie zum Beispiel Videoüberwachung, GPS-/Ortungssysteme, Fingerabdruck- oder Iriserkennungssysteme) sowohl im Unternehmensalltag, als auch zum Schutz ihrer Betriebs-/Geschäftsgeheimnisse oder ihres Eigentums.

Alle diese Vorgänge bergen erhebliche Gefahren und machen deutlich, dass die persönlichen Daten von Beschäftigten außerordentlich missbrauchsanfällig sind. Die Rechte der Beschäftigten bei der Verarbeitung ihrer personenbezogenen und personenbeziehbaren Daten müssen deshalb einem besonderen Schutz unterliegen. Gerade im Arbeitsverhältnis, das davon geprägt ist, dass eine Abhängigkeit der Beschäftigten zum Arbeitgeber besteht, müssen klare gesetzliche Regelungen Datenmissbrauch verhindern. Das Beschäftigungsverhältnis ist keine gleichrangige Beziehung und gerade deshalb besonders anfällig für Generaleinwilligungen zur Datenerhebung, -verarbeitung und -nutzung.

Vor diesem Hintergrund gibt es keine Alternative zu einem wirksamen, eigenständigen Beschäftigtendatenschutzgesetz. Nur so kann sichergestellt werden, dass dem Persönlichkeitsrecht der Beschäftigten Rechnung getragen wird. Datenschutz muss dabei den Schutz personenbezogener und personenbeziehbarer Daten von Beschäftigten vor Missbrauch bedeuten. Die Grundsätze des Datenschutzes wie Datensparsamkeit, Transparenz, Datensicherheit und die Unmittelbarkeit der Datenerhebung müssen sich im Beschäftigtendatenschutz wiederfinden und dem besonderen Verhältnis zwischen Arbeitnehmer und Arbeitgeber Rechnung tragen. Daher bedürfen sie einer besonders genauen, an den Rechtssprechungsgrundsätzen orientierten Ausgestaltung.

Eine eigenständige gesetzliche Regelung ist notwendig, um klare und möglichst verständliche Regelungen zu schaffen. Der Schutz vor unzulässiger Datenerhebung, -verarbeitung und -nutzung kann nur in Form übersichtlicher Regelungen verbessert werden.

Als Grundansatz eines Beschäftigtendatenschutzes müssen die Persönlichkeitsrechte und das Recht auf informationelle Selbstbestimmung gewählt werden, die nach der Rechtsprechung des Bundesverfassungsgerichts den Status von Grundrechten haben. Eingriffe in diese Grundrechte dürfen durch die gesetzliche Regelung nur ausnahmsweise erlaubt werden. Dabei dürfen die Persönlichkeitsrechte der Beschäftigten auch nicht in Abwägung zu unternehmerischen Interessen gestellt werden.

Allein mit Hilfe eines eigenständigen, dem Wandel der Technik angepassten und bereits im Ansatz an Grundrechte anknüpfenden Datenschutzrechts für Beschäftigte können Datenskandale der Vergangenheit verhindert werden. Die Vorfälle bei Lidl und anderen Discountern, die eine Überwachung der Beschäftigten mittels Videokameras bis in die Umkleideräume praktizierten, die Telefonbespitzelung bei der Deutschen Telekom AG oder die Weitergabe von Kundendaten bei der Deutschen Bahn AG haben gezeigt, dass die Hemmschwelle, Persönlichkeitsrechte zu verletzten, sehr niedrig ist. Einer der Gründe dafür sind fehlende oder zu geringe Sanktionsmechanismen, die solche Vorgehensweisen als nicht verwerflich erscheinen lassen. Zudem wird die Rechtsdurchsetzung von Einzelnen dadurch erschwert, dass das aktuell gültige Beschäftigtendatenschutzrecht keinen kollektiven Schutz in Form einer Verbandsklage enthält. Mit Hilfe dieser Mechanismen erhält die digitale Gesellschaft einen effektiven und schutzorientierten Datenschutz, der modernen, demokratischen Werten entspricht, die für eine Gesellschaft im 21. Jahrhundert unverzichtbar sind.

4.2 Sondervoten zu Kapitel 3 *Handlungsempfehlungen*

4.2.1 Sondervoten der Fraktionen CDU/CSU und FDP sowie der Sachverständigen Prof. Dr. Hubertus Gersdorf, Prof. Dieter Gorny, Dr. Wolf Osthaus und Dr. Bernhard Rohleder zu Kapitel 3 *Handlungsempfehlungen*

4.2.1.1 Ergänzendes Sondervotum der Fraktionen CDU/CSU und FDP sowie der Sachverständigen Prof. Dr. Hubertus Gersdorf, Prof. Dieter Gorny, Dr. Wolf Osthaus und Dr. Bernhard Rohleder zu 3.2 *Vorgaben für nationalen, europäischen und internationalen Datenschutz*[328]

6. Eine datenschutzrechtliche Folgenabschätzung kann zwar zu einer Förderung des Datenschutzes von Beginn an führen. Sie kann zugleich aber auch zu einem erheblichen bürokratischen Mehraufwand für betroffene Unternehmen führen. Sie sollte daher nur in bestimmten Fällen, in denen sensible Daten verarbeitet werden, oder wenn die jeweilige Verarbeitung mit besonderen Risiken verbunden ist, verbindlich eingeführt werden.

7. Bereits im geltenden europäischen wie auch im nationalen Datenschutzrecht gibt es ein umfassendes System des individuellen Rechtsschutzes. Es ist daher nicht zu erkennen, wie die Einführung eines Verbandsklagerechts zu einer Verbesserung dieses individuellen Rechtsschutzes führen kann. Zudem ist zu bedenken, dass im Datenschutzrecht keine vergleichbare Position des Betroffenen wie im Verbraucherschutzrecht besteht. Schließlich gibt es im Datenschutzrecht gerade kein Verhältnis von Unternehmer und Verbraucher, sondern nur Rechtsbeziehungen zwischen nicht-öffentlichen und öffentlichen Stellen sowie zwischen einzelnen Privatpersonen. Verbandsklagen könnten jedoch, wenn überhaupt, nur in einzelnen Konstellationen zu einer Stärkung der Individualrechte führen. Sie würden im Gegenzug jedoch zu erheblichen Rechtsunsicherheiten bei allen betroffenen Unternehmen führen.

4.2.1.2 Weiteres ergänzendes Sondervotum der Fraktionen CDU/CSU und FDP sowie der Sachverständigen Prof. Dr. Hubertus Gersdorf, Prof. Dieter Gorny, Dr. Wolf Osthaus und Dr. Bernhard Rohleder zu Kapitel 3 *Handlungsempfehlungen*[329]

Koppelungsverbot

Dem Deutschen Bundestag wird empfohlen, am bestehenden Koppelungsverbot in § 28 Absatz 3b BDSG festzuhalten. Die bisherige Regelung verbietet es, den Vertragsschluss von der Angabe personenbezogener Daten abhängig zu machen, wenn ein anderer Zugang zu gleichwertigen Angeboten und Diensten ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist, also wenn Unternehmen eine marktbeherrschende Stellung haben. Sie stellt einen ausgewogenen Ausgleich zwischen den zu berücksichtigenden Interessen der Nutzer und der Unternehmen dar. Eine Ausweitung des Kopplungsverbotes würde letztlich zu einem vollständigen und damit unnötigen, mithin einem unverhältnismäßigen, gesetzlichen Verbot von Diensten führen.

Regulierte Selbstregulierung

Selbstregulierung durch die Wirtschaft ist ein wichtiges Instrument des Datenschutzes. Im Vergleich zur Gesetzgebung ist sie flexibler und kann schneller auf neue Entwicklungen reagieren. Selbstverpflichtungen der Wirtschaft können darüber hinaus das Datenschutzniveau heben, zum Beispiel durch Vorgaben zur Datenvermeidung und Datensparsamkeit. Dort, wo sich die Selbstregulierung im Interesse der Nutzerinnen und Nutzer sowie der Unternehmen bewährt, ist dann ein Handeln durch den Gesetzgeber nicht notwendig.

Eine zentrale Informations- und Widerspruchsstelle, wie sie beispielsweise der Datenschutz-Kodex für Geodatendienste vorsieht und von der – ohne eine zentrale Speicherung – Widersprüche an die jeweiligen Unternehmen weitergegeben werden, erleichtert es den Nutzerinnen und Nutzern, ihr Widerspruchsrecht auszuüben. Für die Beilegung von Streitigkeiten über die Ausübung von Nutzerrechten kann auf dieser Grundlage eine Schlichtungsstelle Datenschutz zur effektiven unbürokratischen Durchsetzung der gesetzlichen Rechte auf Löschung, Sperrung und Widerspruch beitragen. Diese könnte unter Beteiligung von Wirtschaft und Datenschutzverbänden realisiert werden.

Schadensersatzansprüche im Datenschutzrecht

Dem Deutschen Bundestag wird empfohlen, weiter zu beobachten, ob das Sanktionssystem im Datenschutzrecht auch zukünftig effektiven Schutz gewährleistet. Auch ein Wegfall von Antragserfordernissen bei bestimmten Straftaten im Bereich der Datenverarbeitung, die über individuelle Verstöße hinausgehen, kann zu einer Verbesserung in Betracht gezogen werden.

Wenn eine verantwortliche Stelle dem Betroffenen durch eine datenschutzrechtlich unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zufügt, macht sie sich schadensersatzpflichtig. Dem Deutschen Bundestag wird empfohlen, zu evaluieren, inwieweit die Ansprüche praxistauglich sind und sich als Instrument neben Bußgeldern und Sanktionen etablieren. Falls Verbesserungen erforderlich erscheinen und Unterlassungs- sowie Beseitigungsansprüche nicht ausreichen, könnte unter anderem ein Ersatz immaterieller Schäden wie im öffentlichen Bereich auch für den nichtöffentlichen Bereich in die Überlegungen miteinbezogen werden.

---

[328] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu 3.2 an.

[329] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu Kapitel 3 an.

Beschäftigtendatenschutz

Es ist zu begrüßen, dass die Bundesregierung ein Gesetz zur Regelung des Beschäftigtendatenschutzes auf den Weg gebracht hat. Die Regelungen sollten einen Ausgleich zwischen den Interessen der Arbeitnehmer und Arbeitgeber und damit insgesamt eine Verbesserung des Arbeitnehmerdatenschutzes beinhalten. Es sollten nur solche Daten verarbeitet werden, die für das Arbeitsverhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Arbeitsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante Gesundheitszustände beziehen, müssen ausgeschlossen sein.

Der Einsatz von Informations- und Kommunikationstechnologie am Arbeitsplatz ist heute nicht mehr wegzudenken. Das Spannungsverhältnis zwischen den Interessen von Arbeitnehmern und Arbeitgebern muss vor allem beim Einsatz von webbasierten Kontrollinstrumenten und im Rahmen der gestatteten auch privaten Nutzung betrieblicher Telekommunikationsmittel praxisgerecht und rechtsklar ausgestaltet werden. Hierfür sollte eine eigenständige Regelung getroffen werden. Es muss jedoch auch Raum für Betriebsvereinbarungen und Einwilligungen als unmittelbares, gestalterisches Mittel von spezifischen Gegebenheiten vor Ort bleiben, wobei das aktuell bestehende Schutzniveau nicht unterschritten werden darf.

Datenschutz und Internet der Dinge

Mit der flächendeckenden Einführung des Internetprotokolls IPv6 wird die bisher vorhandene Beschränkung von IP-Adressen auf 4,3 Milliarden Adressen aufgehoben. Zukünftig stehen 340 Sextillionen Adressen allen Nutzerinnen und Nutzern im Internet zur Verfügung. Schon heute zeichnet sich ab, dass sich hierdurch ein Internet der Dinge oder auch „Smart Life“ entwickeln kann. Immer mehr elektronische Geräte (zum Beispiel Kühlschränke) sowie Garagen und Autos können über lokale oder auch überregionale Netzwerke verbunden und so elektronisch gesteuert werden. Diese technologische Weiterentwicklung stellt auch besondere Anforderungen an den Datenschutz, da für das Internet der Dinge insbesondere personenbezogene Verbrauchs- und Gewohnheitsdaten von besonderer Bedeutung sind. Es wird daher angeregt, bereits zu Beginn der Einführung von Smart-Life-Anwendungen durch die Anbieter für eine Vertrauenskultur bei Nutzerinnen und Nutzern zu werben. Dies setzt zunächst voraus, dass datenschutzrechtliche Grundsätze auch hier beachtet werden.

Geodaten und Geolocating

Geodaten werden sowohl von öffentlichen Stellen (im Rahmen von INSPIRE[330]) als auch von nicht-öffentlichen Stellen (zum Beispiel Google Street View und Microsoft Streetside) erhoben und zum Teil im Internet der Öffentlichkeit zur Verfügung gestellt. Dabei ist zu beachten, dass Geodaten allein keine personenbezogenen Daten sind. Durch ihre Personenbeziehbarkeit und die Möglichkeit, sie mit personenbezogenen Daten zu verknüpfen, können sie jedoch datenschutzrechtlich relevant werden. Zudem sind sie aufgrund ihrer zunehmenden Detailschärfe und vielseitigen Einsetzbarkeit eine beliebte, zumeist kostenlose Informationsquelle, die sowohl von Unternehmen als auch von Privatpersonen genutzt und in bestehende Angebote integriert wird.

Durch die gestiegene Verbreitung der Geodatendienste haben sich vielfältige Abgrenzungsfragen der Personenbeziehbarkeit von Daten, aber auch weitere Folgeprobleme, wie zum Beispiel der nicht einvernehmlichen Löschung von Geodaten zu speziellen Objekten, ergeben. Dem Deutschen Bundestag wird daher empfohlen, diese Problematik in seine Überlegungen über gesetzliche Änderungen des Bundesdatenschutzgesetzes miteinzubeziehen.

Geolokalisationsdienste zeichnen sich demgegenüber dadurch aus, dass Daten über die Position der Nutzerin beziehungsweise des Nutzers von mobilen Geräten übertragen werden. Eine Auswertung dieser Daten erlaubt die Erstellung von umfassenden Bewegungsprofilen. Nach dem geltenden Recht sind solche Dienste nur mit Einwilligung des Nutzers zulässig (vergleiche § 4a BDSG). Dem Deutschen Bundestag wird empfohlen, an dieser Regelung weiter festzuhalten und durch einen stringenten Vollzug der gesetzlichen Vorgaben sicherzustellen, dass die Nutzerinnen und Nutzer vor einer Erhebung von personenbezogenen Daten hierüber auch umfassend informiert wurden. Dies gilt insbesondere für den Fall, dass die Daten nicht lediglich zur technischen Durchführung des Dienstes anfallen, sondern darüber hinaus genutzt werden sollen.

4.2.2 Sondervoten der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie verschiedener Sachverständiger zu Kapitel 3 *Handlungsempfehlungen*

4.2.2.1 Ergänzendes Sondervotum der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie der Sachverständigen Constanze Kurz und Annette Mühlberg zu 3.2 *Vorgaben für nationalen, europäischen und internationalen Datenschutz*[331]

Über die gemeinsam beschlossenen Handlungsempfehlungen hinaus wird dem Deutschen Bundestag empfohlen:

Die zunehmende grenzüberschreitende Vernetzung und Globalisierung von Kommunikationsinfrastrukturen macht eine Abstimmung und Modernisierung auch auf supra- wie internationaler Ebene notwendig. Zusätzlichen

---

330 Infrastructure for Spatial Information in the European Community (Geodateninfrastruktur in der Europäischen Gemeinschaft).

331 Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu 3.2 an.

Anlass auf EU-Ebene bieten die Änderungen durch den Lissabon-Vertrag und die Inkorporation der Grundrechtecharta, darunter das Grundrecht auf Datenschutz. Vor diesem Hintergrund ist der Reformansatz der EU-Kommission zu begrüßen.

Dem Deutschen Bundestag wird empfohlen,

die Bundesregierung aufzufordern, sich für eine umfassende Novellierung der Datenschutzrichtlinie einzusetzen, bei der auch der öffentliche Sektor einschließlich der Sicherheitsbehörden in die Harmonisierung einbezogen werden sollte. Regelungen insbesondere zu Privacy by Design, zum Profiling sowie zum Daten- und Personenbezugsbegriff müssen neu geschaffen beziehungsweise vorhandene Regelungen grundlegend überarbeitet werden. Die Revision der Richtlinie muss dabei insbesondere den Herausforderungen der digitalen Gesellschaft, wie zum Beispiel dem Cloud-Computing Rechnung tragen.

4.2.2.2 Ergänzendes Sondervotum der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie der Sachverständigen Constanze Kurz und Annette Mühlberg zu 3.4 *Einwilligung*[332]

Über die gemeinsam beschlossenen Handlungsempfehlungen hinaus wird dem Deutschen Bundestag empfohlen,

in Rechtsbeziehungen, in denen von einer wirklich freien Einwilligungsentscheidung nicht ausgegangen werden kann, weil die betroffene Person nicht dieselbe Machtposition hat wie ihr Gegenüber (also zum Beispiel die öffentliche Stelle beziehungsweise der Internetdiensteanbieter gegenüber dem Nutzer) eine Einwilligung nur dort zuzulassen, wo ihre Erteilung ebenso wie ihre Ablehnung im freien Ermessen der betroffenen Person steht.

4.2.2.3 Ergänzendes Sondervotum der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie der Sachverständigen Constanze Kurz und Annette Mühlberg zu 3.9 *Soziale Netzwerke*[333]

Die Enquete-Kommission hat in ihrem Bericht herausgearbeitet, dass es in sozialen Netzwerken zahlreiche Besonderheiten und Probleme im Umgang mit Daten und Informationen durch die Betreiber der Plattformen gibt.

Über die gemeinsam beschlossenen Handlungsempfehlungen hinaus wird dem Deutschen Bundestag deshalb weiterhin empfohlen,

1. die Betreiber sozialer Netzwerke zu verpflichten, höchstmögliche Sicherheitsvorkehrungen zu treffen, um ein unberechtigtes Kopieren von Daten und Systemeinbrüche zu vermeiden. Regelmäßige Kontrollen, die Nutzung aktueller und effektiver Technologien sowie der Vorrang des Schutzes der Nutzerdaten vor dem Komfort sind dabei zu gewährleisten. Technische Neuerungen müssen vor ihrer Einführung von den Plattformbetreibern auf ihre Auswirkungen auf den Schutz der Daten und Inhalte der Mitglieder umfassend geprüft werden,
2. den Anbietern zu untersagen, die Nutzungsmöglichkeit von sozialen Netzwerken an eine Einwilligung in die über die Erfüllung des Vertragszwecks hinausgehende Datennutzung zu koppeln,
3. einen gesetzlichen Anspruch der Nutzerinnen und Nutzer sozialer Netzwerke auf Löschung des Accounts inklusive aller gespeicherter Nutzerdaten zu schaffen. Dies entspricht den datenschutzrechtlichen Vorgaben. Eine bloße Deaktivierung des Accounts als einzige Option der Abmeldung ist nicht ausreichend, da hierbei alle Daten weiterhin gespeichert bleiben und der Account samt der vorhandenen Daten jederzeit wieder aktiviert werden kann. Die Löschung des Accounts muss für die Nutzer ohne Hürden möglich sein. Die Löschungspflicht der Daten sollte gesetzlich verankert werden,
4. die Anbieter sozialer Netzwerke zu verpflichten, in einer verständlichen Formulierung der Nutzungs- und Datenschutzbestimmungen die Nutzer über die möglichen Risiken der Nutzung sozialer Netzwerke aufzuklären,
5. die Betreiber zu verpflichten, bei der Neuanmeldung in einem sozialen Netzwerk die Datenerhebung auf ein Minimum der für die Anmeldung erforderlichen Daten beschränken. Ein Recht auf pseudonyme Nutzung sollte ebenfalls gewährleistet sein,
6. die Anbieter sozialer Netzwerke zu verpflichten, die Voreinstellungen der Nutzerprofile auf das Minimum der für die Nutzung des Netzwerks notwendigen Daten zu beschränken, sodass Nutzerinnen und Nutzer sich aktiv für die Freigabe ihrer Daten entscheiden können. Da sich gezeigt hat, dass Datenschutzinformationen bei der Anmeldung zu einem sozialen Netzwerk selten gelesen werden, empfiehlt es sich, dass während der Nutzung des Dienstes eingebaute, kontext-sensitive Funktionen Nutzerinnen und Nutzer über die möglichen Konsequenzen ihres Handelns informieren, etwa wenn sie Datenschutzeinstellungen verändern,
7. die Anbieter sozialer Netzwerke zu verpflichten, bei der Umsetzung von Programmierschnittstellen für externe Anwendungen, die so genannten Apps, dafür Sorge zu tragen, dass Dritte nur mit einer aktiven und informierten Einwilligung der Nutzerinnen und Nutzer auf Daten zugreifen können. Die Betreiber der sozialen Netzwerke haben ebenfalls dafür Sorge zu tragen, dass die Schnittstelle von Netzwerk und externer An-

[332] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu 3.4 an.
[333] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu 3.9 an.

wendung nicht zum Missbrauch genutzt werden kann. Auch die Daten Dritter, wie von „Freunden“ der die externe Anwendung nutzenden Person, dürfen über die Schnittstelle nicht ohne explizite Einwilligung der betroffenen Person preisgegeben werden.

4.2.2.4 Ergänzendes Sondervotum der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie der Sachverständigen Constanze Kurz und Annette Mühlberg zu 3.10 *Datenschutzaufsicht*[334]

Über die gemeinsam beschlossenen Handlungsempfehlungen hinaus werden die auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geforderten nachfolgenden gesetzgeberischen Maßnahmen unterstützt. Es wird empfohlen,

1. dafür Rechnung zu tragen, dass eine wirksame Kontrolle zur Voraussetzung eines erfolgreichen Datenschutzes wird. Wenn man Datenschutz zudem zunehmend als Querschnittsaufgabe begreifen will, muss dies auch institutionelle Folgen haben. Um die – auch von der Datenschutzrichtlinie geforderte und vom EuGH bestätigte – vollständige Unabhängigkeit der Datenschutzinstanzen zu stärken und um Interessenkonflikte zu vermeiden, sollte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit weder dem Bundesministerium des Innern noch einer anderen Bundesbehörde zugeordnet sein. Er sollte frei von Rechts- oder Fachaufsicht seiner Aufsichtstätigkeit nachgehen können. Eine Dienstaufsicht ist allenfalls in eingeschränkter Form zulässig,
2. das Urteil des EuGH[335] zu berücksichtigen und die gesetzlichen Grundlagen für die Unabhängigkeit der Kontrollstellen im Sinne der Datenschutzrichtlinie umzusetzen,
3. dafür zu sorgen, dass § 38 BDSG dahingehend überarbeitet wird, dass
   - das Anordnungsrecht gemäß § 38 Absatz 5 BDSG effektiver ausgestaltet und den üblichen Grundsätzen des Verwaltungsvollzugs angepasst wird,
   - eine gesetzliche Mitwirkungspflicht der kontrollierten Stelle gegenüber der Aufsichtsbehörde geschaffen wird, ähnlich der Mitwirkungspflicht im Sinne des § 24 Absatz 4 BDSG oder des § 5 des Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung,
4. dafür zu sorgen, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die den Länderbehörden zustehenden Anordnungsbefugnisse in entsprechender Weise für alle Bereiche, in denen er die Aufsicht führt, also auch für die Aufsicht über die nicht-öffentlichen Stellen nach dem Telekommunikationsgesetz sowie dem Postgesetz[336] erhält,
5. die Ausdehnung der Zeugnisverweigerungsrechte und Beschlagnahmeverbote auf Informationen und Unterlagen, die die Aufsichtsbehörden bei Berufsgeheimnisträgerinnen und -trägern erlangt haben, gesetzlich zu regeln,
6. eine Strafantragsbefugnis für die Datenschutzaufsichtsbehörden in § 205 StGB festzulegen.

4.2.2.5 Ergänzendes Sondervotum der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie der Sachverständigen Annette Mühlberg zu 3.11 *Vorbildwirkung öffentlicher IT-Projekte*[337]

Über die gemeinsam beschlossenen Handlungsempfehlungen hinaus wird der Bundesregierung empfohlen,

1. bei öffentlichen IT-Projekten der Vorbildwirkung gerecht zu werden und auf ein besonders hohes Schutzniveau zu drängen. Dabei ist auf weitere Datensammelprojekte großen Umfangs zu verzichten, die Kritik der Datenschützer ernst zu nehmen und in eine breite gesellschaftliche Debatte mit staatlichen und nicht staatlichen Akteuren zu treten,
2. die genannten Projekte einer erneuten Prüfung zu unterwerfen, die insbesondere die technischen Grundlagen einer ergebnisoffenen datenschutzrechtlichen Evaluation zugänglich macht. E-Government-Angebote im Bereich der Dienstleistungen für Bürgerinnen und Bürger müssen den aktuellsten technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz genügen,
3. eine stärkere aktive Einbeziehung datenschutzrechtlicher Aspekte in alle Planungsetappen im Bereich des verwaltungsübergreifenden Arbeitens sicherzustellen, weil dies eine besondere Herausforderung in datenschutzrechtlicher Hinsicht darstellt. Dies insbesondere mit dem Ziel, national wie international, bei Offshoring und Outsourcing einen unsensiblen Umgang mit Datenschutzbelangen frühzeitig zu verhindern,
4. bei zentralen IT-Projekten, auch jenen, die von der EU eingeleitet werden, den Datenschutz bereits von Beginn an in der Konzeption zu berücksichtigen,
5. beim Einkauf komplexer Standardprodukte wie Zeiterfassungs- oder Zugangskontrollsysteme für öffentliche Einrichtungen sicherzustellen, dass die erfassten Daten tatsächlich nur im Rahmen ihrer Zweckbestimmung verwertet werden. Wenn Aufträge für die Entwicklung solcher Projekte vergeben werden, sollten sie stets die Programmierung entsprechender technischer Begrenzungen beinhalten. Im Interesse der Ver-

[334] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu 3.10 an.
[335] EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland.
[336] Postgesetz vom 22. Dezember 1997, BGBl. I S. 3294, zuletzt geändert durch Verordnung vom 31. Oktober 2006, BGBl. I S. 2407.
[337] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu 3.11 an.

wirklichung möglichst vorbildlichen Datenschutzes sollte dies bereits bei der finanziellen Planung berücksichtigt werden,

6. in Ämtern und Behörden wegen des erhöhten Einsatzes von Software und des Zugriffs hierauf durch verschiedene Mitarbeiter Vorkehrungen zu treffen, die eine Verletzung insbesondere des Sozialdatenschutzes ebenso ausschließen wie des Steuergeheimnisses,

7. dafür Sorge zu tragen, dass in den kommenden fünf Jahren mindestens 10 Prozent der Forschungsgelder aus dem Bereich IT in Bereichen der Datenschutztechnologien gebunden werden. Über die Verwendung der Gelder sollte nach Beratung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der geplanten Stiftung Datenschutz und Interessenvertretern der betroffenen Akteure entschieden werden.

4.2.2.6 Sondervotum der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN sowie der Sachverständigen Annette Mühlberg zu 3.13 bis 3.21[338]

Hintergrund und Ausgangslage

Maßgeblicher Ausgangspunkt für die Notwendigkeit datenschutzrechtlicher Reformen waren und sind die tiefgreifenden Veränderungen der Informations- beziehungsweise Kommunikationstechnologien sowie die damit einhergehenden Veränderungen der Angebote und Dienste, des Nutzungsverhaltens und insbesondere des Verhaltens der datenverarbeitenden Stellen. Die letzte größere Reform des Datenschutzrechts erfolgte Ende der 1990er Jahre zu einer Zeit, als beispielsweise das Internet sich noch in einer ersten Aufbruchsphase befand, dort vollkommen andere Anwendungen und Technologien zum Einsatz kamen und es nicht annähernd die heutigen Nutzerzahlen aufwies. Grundlegende und nach wie vor geltende Regelungselemente des Datenschutzrechts basieren auf der Vorstellung der Großrechnertechnologie und der Rechenzentren der 1970er Jahre.

Mittlerweile hat sich eine wesentlich veränderte Informations- und Kommunikationsgesellschaft herausgebildet. Das weltweite Internet ist zur zentralen Kommunikationsinfrastruktur moderner Nationalstaaten aufgerückt. Zu den prägenden Entwicklungen auf der technischen Seite wie auch auf der Seite der Anwender zählen etwa – unter stetiger Reduktion der Kosten – weiter ansteigende Rechnerkapazitäten, Miniaturisierung, verbesserte Chip- und Mikroprozessortechnologien, die Ausweitung der Netztechnologie, Profiling-Technologien sowie die mobilen Anwendungen. Die heute zentralen Angebote des Internets, welche unter dem Schlagwort Web 2.0 zusammengefasst werden, sind durch interaktive Dienste gekennzeichnet. Damit gewinnen der „User“ und sein Verhalten, vor allem seine eigene Datenverarbeitungspraxis, an Bedeutung.

[338] Soweit sich die Sachverständige Constanze Kurz diesem Sondervotum in Teilen anschließt, ist dies durch eine Fußnote an der entsprechenden Textpassage kenntlich gemacht.

Geprägt werden das Internet wie auch der Mobilfunkmarkt zudem durch oligopolistische Strukturen, sodass einige wenige Unternehmen maßgeblichen Einfluss auf zentrale Entwicklungen ausüben. Die Verarbeitung von Daten und Informationen insbesondere zum Zweck der personalisierten Werbeansprache strukturiert die Geschäftskonzepte der größten Webunternehmen. Quantität wie auch Qualität der Datensammlungen in den Händen privater Stellen haben in den vergangenen Jahren exponentiell zugenommen und sind unter anderem auch für staatliche Stellen von weiter wachsendem Interesse. Das belegen die Debatten um die Einführung verpflichtender Speicherungen von Telekommunikationsverkehrsdaten, von Finanztransaktionsdaten wie auch von Flugpassagierdaten.

In wichtigen gesellschaftlichen Bereichen wie dem Internet, der Telekommunikation, bei Mobilität und Verkehr, den öffentlichen Räumen des täglichen Lebens oder bei Finanz- und Geldgeschäften hat die Digitalisierung dazu geführt, dass das Verhalten von Bürgern registriert, gespeichert und zumindest nachträglich für zunehmend länger zurückliegende Zeiträume nachvollzogen werden kann. Zudem steht die Gesellschaft erst heute, allerdings nun tatsächlich, vor dem Eintritt in das bereits 2000 im damaligen Modernisierungsgutachten[339] etwas vorschnell prognostizierte Ubiquitous Computing, die so genannte allgegenwärtige Datenverarbeitung. Darauf deuten zunehmend geodatengestützte Anwendungen, erste marktgängige Nutzungen von RFID[340]-Chips, die weit verbreitete Videoüberwachung, die Telematik im Automobilsektor oder auch das in Zukunft realisierte Smart Grid/Metering im Energiesektor hin. Damit steht der Datenschutz heute vor der Situation, dass ganze Infrastrukturen erfassbar und auswertbar werden. Eine verkürzte, allein auf die Vorstellung eines eigentumsanalogen Verfügungsrechts verengte Schutzperspektive wird dieser veränderten Risikolage nicht gerecht. Umfang und Qualität der Datenverarbeitung haben vielmehr massive, auch gesamtgesellschaftliche Auswirkungen. Die damit verbundenen überindividuellen Risiken etwa des Missbrauchs von Daten, des damit einhergehenden breiten Vertrauensverlustes bei Nutzerinnen und Nutzern sowie der möglichen Vermeidung der Nutzung ganzer Kommunikationsinfrastrukturen sind konzeptionell bislang nicht hinreichend berücksichtigt.

Der Reformstau im Bereich des Datenschutzes ist weitgehend unbestritten. Die Modernisierung des Datenschutzes führte bereits 1998 zur Befassung des Deutschen Juristentages, der weitreichende Änderungsvorschläge unterbreitete. Die damalige Bundesregierung beabsichtigte eine zweistufige und grundlegend ansetzende Reform. Realisiert wurde lediglich die erste Stufe in Gestalt der Umsetzung der dringlichsten Anforderungen der Datenschutzrichtlinie. Der durch ein umfangreiches wissen-

[339] Vgl. Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern. 2002. Online abrufbar unter: www.computerundrecht.de/media/gutachten.pdf

[340] Radio Frequency Identification.

schaftliches Gutachten[341] vorbereitete zweite Reformschritt konnte nicht mehr verwirklicht werden. Seit 2009 hat auch die Europäische Kommission die Reform der Datenschutzrichtlinie angekündigt, Konsultationen in den Mitgliedstaaten durchgeführt sowie Ende 2010 erste Eckpunkte einer Reform vorgelegt, die neben dem Bereich der Privatwirtschaft auch eine Harmonisierung der staatlichen Datenverarbeitung, insbesondere bei den Polizei- und Justizbehörden der Mitgliedstaaten, herbeiführen soll.

Die gesellschaftliche Reaktion auf die genannten Veränderungen fällt in Deutschland recht deutlich aus. In Umfragen wünscht sich eine klare Mehrheit der Bundesbürger einen verbesserten Schutz ihrer Daten. Die Ausweitung des Internethandels gilt durch Vertrauensdefizite in der Bevölkerung zumindest als belastet. Denn viele Bürger fürchten sich vor dem Missbrauch ihrer personenbezogenen Daten, besonders bei der Nutzung des Internets. Anstrengungen beim Datenschutz hingegen können die Akzeptanz für neue Technologien erhöhen und das Vertrauen in deren Nutzung stärken.

Eine Gruppe von besonders internetaffinen Nutzern hat auch außerhalb Deutschlands eine „Postprivacy“-Debatte angestoßen, die den Wert des Datenschutzes im Internetzeitalter neu thematisiert. Kernaussage ist dabei die eher empiristische These vom Kontrollverlust hinsichtlich der Daten im Internet. Weil es im Kontext des Internets faktisch nicht mehr möglich sei, im Wege des Selbstschutzes eigene Daten vor der Weiterverarbeitung durch Dritte zu schützen, habe sich der Datenschutz überlebt und werde einer neuen Kultur der Transparenz weichen. Dem wird in der öffentlichen Debatte allerdings entgegengehalten, es handele sich um einen Fehlschluss, weil aus dem so beschriebenen Sein allein kein Sollen ableitbar sei. Auch gilt die These vom Kontrollverlust schon deswegen als wenig zielführend, weil sie ein verkürztes Schutzprogramm des Datenschutzes beschreibt, bei dem aufgrund der Fehlvorstellung eines ausschließlich individuellen Verfügungsrechts primär Elemente des Selbstdatenschutzes dem Datenschutz zugerechnet werden. Allerdings besteht Datenschutz längst aus einer Vielzahl von weit darüber hinausgehenden Schutzvorkehrungen und Maßnahmen.

Die massive Zunahme der Verarbeitung personenbezogener Daten in einem zunehmend unübersichtlicheren Feld von Akteuren fordert vom Gesetzgeber eine konsequente Neuausrichtung des Regelungsfeldes. Der bestehende ordnungsrechtliche Regelungsansatz, wie er insbesondere im Bundesdatenschutzgesetz sowie dem Telemediengesetz und Telekommunikationsgesetz zum Ausdruck kommt, ist nicht grundsätzlich obsolet geworden. Ein allgemeiner Rückzug auf Selbstregulierungen, wie er zum Teil etwa mit Blick auf Fragen des Internetdatenschutzes vorgeschlagen wird, verfehlt jedoch die Vorgaben der verfassungsgerichtlichen Rechtsprechung zur mittelbaren Drittwirkung sowie den grundrechtlichen Schutzpflichten. Andererseits bedarf es einer sachgerechteren Beurteilung und Behandlung von Datenschutzfragen vor Ort bei den verarbeitenden Stellen selbst. Dem entspricht eher die Orientierung an Konzepten regulierter Selbstregulierung beziehungsweise Koregulierung. Es bedarf auch weiterhin klarer Vorgaben hinsichtlich der Zulässigkeit bestimmter Datenverarbeitungen, verbunden mit eben so deutlichen Regelungen zu den Konsequenzen von Verstößen. Die Durchsetzung dieser Regelungen muss durch ein unabhängiges und effizientes Aufsichtssystem gewährleistet sein. Nicht zuletzt das Bundesverfassungsgericht sieht dieses Ordnungssystem als maßgeblich an, weil der Umgang mit personenbezogenen Daten und Informationen zu einem großen Teil dem Schutzbereich insbesondere des Grundrechts auf informationelle Selbstbestimmung unterfällt. Hinsichtlich der Zielsetzung des Datenschutzes ist bedeutsam, dass sich aus dem Grundrecht auf informationelle Selbstbestimmung eine Vielzahl unterschiedlicher Schutzerfordernisse ergibt.

Daten und Informationen

Sachangemessene Regelungen bedürfen einer differenzierten begrifflichen Beschreibung. Die bisherige Verwendung der Begriffe Daten und Informationen greift zu kurz. Daten sind Zeichen, die auf Datenträgern vergegenständlicht festgehalten werden und als Informationsgrundlagen dienen. Informationen selbst hingegen werden als Sinnelemente erst in bestimmten sozialen Verwendungszusammenhängen durch aktive Deutungsleistungen (sozialer Kontext) erzeugt und genutzt.[342] Mit dieser Unterscheidung wird die im Datenschutz durchaus bekannte „Kontextabhängigkeit“ für die Bewertung der mit Datenverarbeitungen verbundenen Risiken besser herausgearbeitet. In der Folge wird es möglich, zusätzliche Anknüpfungspunkte für präzisere Schutzmaßnahmen zu formulieren. Zukünftig sollte die Unterscheidung von Daten und Informationen deshalb vom Gesetzgeber besser herausgearbeitet werden.

Anwendungsbereich/Personenbezug

Bei der Reform des Datenschutzes ist zu berücksichtigen, dass der grundlegende Ansatz des Datenschutzrechts, nämlich die Personenbezogenheit eines Datums, in der digitalen Welt weiterentwickelt werden muss. Zwar ist auch im Internet nicht jedes Datum personenbezogen, doch grundsätzlich sind alle Daten personenbeziehbar. Es gibt kein belangloses Datum mehr. Denn durch die Verknüpfung mit anderen Daten kann ein Personenbezug jederzeit hergestellt werden. Das bedeutet vor allem, dass Daten nicht von vornherein aus dem Schutz herausfallen dürfen. Es kommt mehr denn je darauf an, einen abgestuften gefährdungsabhängigen Schutz zu entwickeln, damit

[341] Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern. 2002. Online abrufbar unter: www.computerundrecht.de/media/gutachten.pdf

[342] Vgl. Albers, Marion: Umgang mit personenbezogenen Daten und Informationen. 2008, § 22.

der Anwendungsbereich des Datenschutzrechts nicht beliebig weit geöffnet und damit konturlos wird.

Die technischen Möglichkeiten der Verkettung verschiedener Datensätze haben sich grundlegend erweitert. Dem muss die zukünftige gesetzgeberische Gestaltung Rechnung tragen.

Abwehr- und Schutzkomponente

Datenschutz beinhaltet verfassungsrechtlich gesehen weit mehr als eine bloße Abwehr von Eingriffen in das Recht auf informationelle Selbstbestimmung. Die Schutzkomponenten betreffen nicht nur das Verhältnis zum Staat, sondern aufgrund konkreter Gefahren der personenbeziehbaren Datenverarbeitung auch den Bereich der Privatwirtschaft. Im Sinne der Gewährleistung einer freien Persönlichkeitsentfaltung der Bürgerinnen und Bürger beinhaltet die Schutzkomponente des Datenschutzes deshalb auch eine staatliche Verpflichtung, Maßnahmen zu treffen, die gewährleisten, dass die Daten des Einzelnen wirksam geschützt sind und dass er über die Verarbeitung dieser Daten informiert wird.

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme/ Grundrecht auf informationelle Selbstbestimmung[343]

Angesichts der Bedeutung des Schutzes der personenbezogenen Daten für nahezu alle Lebensbereiche und der wegweisenden Rechtsprechung des Bundesverfassungsgerichts, insbesondere mit Blick auf die zukünftige technische Entwicklung, wird dem Deutschen Bundestag empfohlen zu prüfen,

1. ob die vom Bundesverfassungsgericht geschaffenen Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in den Grundrechtekatalog des Grundgesetzes als eigenständig formulierte Grundrechte aufgenommen werden sollten,
2. ob es der Fortentwicklung des Post- und Fernmeldegeheimnisses nach Artikel 10 GG hin zu einem übergreifenden Recht auf Schutz des Kommunikationsgeheimnisses bedarf.

Grundprinzipien des Datenschutzrechts/Änderungsbedarf Bundesdatenschutzgesetz (Modernisierung, Vereinfachung, Sprache)

Die Grundprinzipien des deutschen Datenschutzes wurden in Kapitel 2.1 dieses Berichts dargestellt. Wie die Enquete-Kommission in ihrer Beschreibung jedoch feststellt, werden diese Prinzipien in vielen Konstellationen nicht beachtet beziehungsweise nachrangig zu anderen Interessen gestellt.

Deshalb werden dem Deutschen Bundestag nachfolgende Handlungsempfehlungen gegeben:

1. die ins Stocken gekommene Modernisierung des unübersichtlichen Datenschutzrechts fortzusetzen. Das Ziel der Modernisierung muss eine deutliche Vereinfachung und Integration datenschutzrechtlicher Bestimmungen sein, wobei das bestehende Schutzniveau nicht abgesenkt werden darf. Dieses Ziel wird nur dann verwirklicht werden können, wenn das geltende Datenschutzrecht um neue Datenschutzinstrumente ergänzt wird. Hierbei wird der Implementierung eines Datenschutzes durch Technik große Bedeutung zukommen,
2. zu überprüfen, inwieweit es einer Weiterentwicklung der Grundbegriffe und der bestehenden Dogmatik des Datenschutzrechts bedarf, insbesondere im Hinblick auf eine bessere Abgrenzung der Begriffe Daten, Informationen und Wissenskontext sowie die der sich daraus ergebenden Konsequenzen. Dies ist geboten, weil ein allein auf Daten bezogenes und individualistisches Verständnis des Datenschutzrechts unsachgerecht schutzverkürzend wirken kann,
3. ein allgemeines, nicht subsidiäres Gesetz für einen modernen Datenschutz zu verabschieden, das unter Vermeidung von Doppelregelungen eine klare Abgrenzung zwischen allgemeinen und bereichsspezifischen Regelungen erlaubt. Wenn möglich, soll es zu einem Verzicht, jedenfalls zu einer Reduzierung, bereichsspezifischer Regelungen führen. Das Gesetz soll darüber hinaus auch allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten. Zudem soll es weitaus stärker auf die bereits im Gesetz verankerten Grundprinzipien Datensparsamkeit und Datenvermeidung setzen,
4. bei der Erarbeitung eines allgemeinen Datenschutzgesetzes die zur Verwirklichung der informationellen Selbstbestimmung wesentlichen Schutzziele, wie Datensparsamkeit und Datenvermeidung, Datensicherheit, Zweckfestlegung und -bindung, Systemdatenschutz, Transparenz, Gestaltungsrechte (Auskunfts-, Widerspruchs-, Benachrichtigungs-, Korrektur- und Löschungsrechte), Nichtverkettbarkeit (als technische Sicherung der Zweckbindung) sowie Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte)[344], als übergreifende Grundprinzipien voranzustellen,
5. dass die allgemeinen Datenschutzgrundsätze gleichermaßen für den öffentlichen und für den nicht-öffentlichen Bereich gelten sollten,

[343] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[344] Vgl. hierzu auch Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile

6. den Zweckfestlegungs- beziehungsweise Zweckbindungsgrundsatz in Verbindung mit dem Erforderlichkeitsgrundsatz durch eine eigene Norm hervorzuheben und zu konkretisieren. Dabei sollten auch Vorgaben für die Änderung bei Zweckfestlegung und Zweckbindung klar geregelt sein. In diesem Zusammenhang müssen Regelungen erarbeitet werden, nach denen es Nutzerinnen und Nutzern möglich ist, auch in der vernetzten Welt die Kontrolle über die Verwendung ihrer persönlichen Daten ausüben zu können,

7. zu prüfen, inwieweit Sanktionen bei Verstößen gegen den Zweckfestlegungs- beziehungsweise Zweckbindungsgrundsatz eingeführt werden sollten. Den Aufsichtsbehörden muss ermöglicht werden, gegen Unternehmen, die nachgewiesenermaßen anlasslos oder zweckwidrig Daten erheben, speichern, verarbeiten und nutzen, wirkungsvolle Sanktionen zu verhängen. In diesem Zusammenhang ist die bereits im BDSG verankerte Löschungspflicht zu betonen. Ein Verwertungsverbot für Daten, die durch rechtswidrige Änderung des ursprünglichen Erhebungszwecks erlangt worden sind, sollte gesetzlich verankert werden. Regelungsbedarf besteht etwa im Hinblick auf die Verwertung von unrechtmäßig erlangten Daten in Gerichtsprozessen,

8. dass die Informationspflichten privater Anbieter gegenüber Nutzerinnen und Nutzern erweitert und die Auskunftsansprüche der Nutzerinnen und Nutzern gegenüber Anbietern gestärkt werden,

9. die Informationspflichten sowohl öffentlicher als auch nicht-öffentlicher Stellen gegenüber den Betroffenen bei Datenpannen zu erweitern,

10. dass, um Unsicherheiten bei der Festlegung der Verantwortlichkeit von vornherein zu vermeiden, die Formulierung „Daten verarbeitende (beziehungsweise speichernde) Stelle“ dem Wortlaut der Europäischen Datenschutzrichtlinie angepasst wird („die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“). Darüber hinaus bedarf es einer gesetzlichen Klärung für die zunehmenden Konstellationen, bei denen eine Vielzahl von Beteiligten die Datenverarbeitung durchführen,

11. die Informationspflichten darüber hinaus wie folgt zu erweitern:

    – durch klare und eindeutige Offenlegung der Verantwortlichkeit für die Datenverarbeitung bei mehreren Stellen gegenüber den Betroffenen,

    – durch prominente Platzierung der datenschutzrechtlich verantwortlichen Stelle und der zuständigen Datenschutzbehörde,

    – durch eine Verpflichtung der verantwortlichen Stelle, Herkunft und Empfänger von Daten zu dokumentieren sowie Datenbankzugriffe zu protokollieren, wenn personenbezogene Daten an Dritte weitergegeben werden,

    – durch eine gesetzliche Festschreibung der Möglichkeit, Widerspruchsrechte ohne Medienbrüche auszuüben. Die Ausübung des Widerspruchsrechts wird von den Anbietern bisweilen absichtlich erschwert. Häufig lassen sie einen Widerspruch gegen die Datenerhebung nur schriftlich zu, während die Einwilligung in die Erhebung durchaus auf elektronischem Wege erteilt werden kann,

12. das so genannte Koppelungsverbot auch auf solche Unternehmen und Dienste auszuweiten, die keine marktbeherrschende Stellung haben. Nach geltender Rechtslage darf der Abschluss eines Vertrages (etwa bei der Nutzung von Internetdiensten) nicht an eine Einwilligung gekoppelt werden, die eine über die Diensterbringung hinausgehende Datenerhebung und -nutzung erlaubt. Dies gilt allerdings nur für solche Unternehmen, die eine marktbeherrschende Stellung innehaben,[345]

13. eine Befassung des Deutschen Bundestages mit der Frage, wie Betroffenenrechte im Bundesdatenschutzgesetz gestärkt werden können (vergleiche §§ 33 ff. BDSG). Dabei sollte dem Einsatz moderner Technologien (etwa dem Recht auf elektronische Auskunft über die gespeicherten Daten und einem elektronischen Widerspruchsrecht) besondere Bedeutung zukommen. Die Auskunftsrechte der Betroffenen sind zu vereinfachen und bürgerfreundlicher auszugestalten,

    – durch entsprechende Bereitstellung technischer Mittel, die die Wahrnehmung der Rechte vereinfachen,

    – durch eine Einführung eines allgemeinen Rechts auf elektronische Auskunft, unter anderem im Hinblick auf die Verknüpfung beziehungsweise Zusammenführung von Daten sowie die über den eigentlichen Zweck der Erhebung hinausgehende Nutzung,

    – durch eine Verpflichtung der Anbieter, Nutzerinnen und Nutzer über Änderungen der für das betreffende Angebot geltenden Datenschutzbedingungen effektiv zu informieren,

14. Konzepte wie den vom Chaos Computer Club (CCC) vorgeschlagenen Datenbrief, der Unternehmen verpflichtet, in regelmäßigen Abständen Bürgerinnen und Bürger über ihre bei den Unternehmen gespeicherten persönlichen Daten zu unterrichten, in die Überlegungen für eine Stärkung der informationellen Selbstbestimmungsrechte einzubeziehen. Der Datenbrief ist kritisch zu bewerten, wenn und soweit damit eine eigene Sammlung und Zusammenführung von Daten zu Personen verbunden ist und ein nicht zu bewältigender Aufwand für die betroffenen Unterneh-

---

[345] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

men droht. Diesen Problemen muss in der Ausgestaltung eines Konzeptes wie des Datenbriefs Rechnung getragen werden,

15. dass das Auskunftsrecht sich auch auf Datenverkettungen beziehen sollte. Welche persönlichen Daten bei einem bestimmten Anbieter mit anderen verknüpft werden und nach welchen Selektionskriterien dies geschieht, können datenschutzbewusste Nutzerinnen und Nutzer derzeit nicht in Erfahrung bringen,

16. sicherzustellen, dass Betroffene, deren personenbezogene Daten an Dritte übermittelt werden, über den tatsächlichen Empfänger ihrer Daten informiert werden müssen. Wenn personenbezogene Daten an Dritte übermittelt werden, muss der Betroffene bislang lediglich über die „Kategorien von Empfängern“ (§ 33 Absatz 1 BDSG) unterrichtet werden. Er erfährt jedoch nicht, wer seine Daten tatsächlich bekommen hat. Dieser Missstand wäre mit einer schlichten Formulierungsänderung im Gesetz leicht zu beheben. Verstöße gegen diese Regelung könnten zudem mit einem Bußgeld belegt werden,

17. die Formulierung einer einheitlichen allgemeinen technikunabhängigen Vorschrift zur transparenten Datenerhebung, -verarbeitung und -nutzung, die unter anderem folgende Punkte regelt:
    - ein grundsätzliches Verbot der unbemerkten Datenerhebung mit Sanktionen im Falle des Verstoßes,
    - eine Informationspflicht gegenüber den Betroffenen über die Funktionsweise und Art der Datenerhebung, die Identität der verantwortlichen Stelle sowie Rechte der Betroffenen,

18. die Schaffung einer allgemeinen, technikunabhängigen Regelung zur Verarbeitung personenbezogener Lokalisierungsdaten unter Verpflichtung der Lokalisierungsdienstanbieter, die konkrete Ortung des Betroffenen durch ein Signal anzuzeigen sowie innerhalb von Tracking-Systemen die Einwilligung des Betroffenen vorzusehen. Der E-Privacy-Richtlinie zufolge ist für die Verarbeitung von Positionsdaten aus GSM/UMTS (Mobilfunk), bei denen es sich stets um Tracking-Systeme handelt, ausdrücklich eine Einwilligung des Betroffenen erforderlich. Bislang ist diese Vorgabe der Richtlinie jedoch nicht in das Bundesdatenschutzgesetz aufgenommen worden. Das Gesetz ist in diesem Punkt deshalb bislang nicht europarechtskonform. Bei der Ausgestaltung ist auf Technikneutralität zu achten. Ferner muss es Betroffenen ermöglicht werden, im Rahmen der technischen Möglichkeiten eine Ortung der eigenen Person zu verhindern. Positionsdaten sollten in die Kategorie der besonders schützenswerten („sensitiven“) Daten ins Bundesdatenschutzgesetz (§ 3 Absatz 9) aufgenommen werden,

19. für die Betroffenen eine Anspruchsnorm mit Sanktionierung bei Nichtbeachtung zu schaffen, die die verantwortliche Stelle dazu verpflichtet, ihre Systeme und Verfahren so auszurichten, dass nur Daten erhoben werden, die auch erforderlich sind,

20. entsprechend der europäischen Datenschutzrichtlinien gleiche Regeln für öffentliche und nicht-öffentliche Stellen zu schaffen und dabei verbindliche datenschutzrechtliche Mindeststandards festzuschreiben. Dies begründet sich, neben zahlreichen weiteren Argumenten, auch in dem als zunehmend problematisch erscheinenden Umgang mit öffentlich zugänglichen personenbezogenen Daten. Darf beispielsweise die Polizei Daten über Demonstrationsteilnehmer in sozialen Netzwerken recherchieren und unbeschränkt miteinander verknüpfen? Personenbezogene Daten, welche aus „allgemein zugänglichen Quellen“ stammen oder vom Betroffenen „zur Veröffentlichung vorgesehen“ sind, dürfen nach derzeitiger Rechtslage erhoben werden. Aufgrund der besonderen Gefahren, die die Erhebung solcher Daten allein schon durch die Möglichkeit der nachfolgenden Verkettung mit sich bringt, erscheint dies unbefriedigend. Die Privilegierung öffentlich zugänglicher Daten sollte auf solche Verwendungen eingeschränkt werden, die im offensichtlichen oder erklärten Interesse des Betroffenen liegen beziehungsweise diesem nicht widersprechen. Die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Regeln im Datenschutz ist nicht mehr zeitgemäß. Zur Einhaltung datenschutzrechtlicher Mindeststandards für den öffentlichen und nicht-öffentlichen Bereich sollten effektive und abschreckende Sanktionen festgelegt werden. Ebenfalls angebracht scheint eine Erweiterung der Bußgeldtatbestände, insbesondere für unbefugte Datennutzung und unzulässige Beobachtung (Videoüberwachung).

Anonymität und Pseudonymität[346]

Die Enquete-Kommission hat in ihrer Bestandsaufnahme festgestellt, dass auch eine anonyme und pseudonyme Nutzung des Internets zur Ausübung des Rechts auf informationelle Selbstbestimmung gehören kann. Deshalb wird dem Deutschen Bundestag empfohlen,

1. durch gesetzgeberische Maßnahmen zur Stärkung der Möglichkeit der anonymen Nutzung elektronischer Medien den Datenschutz zu verbessern,

2. die allgemeine gesetzliche Verpflichtung der Dienstleister, anonyme und pseudonyme Nutzungsmöglichkeiten von Internetdiensten anzubieten, weiter zu stärken. Verstöße gegen die Möglichkeit und Wahrung von Pseudonymität und Anonymität sollten ferner sanktioniert werden können.

Verbandsklage[347]

Dem Deutschen Bundestag wird empfohlen,

eine gesetzliche Regelung zu schaffen, die Verbraucherschutz- und Datenschutzverbänden eine „fremdnützige“

[346] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[347] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

Klagebefugnis einräumt, ähnlich dem Instrument des Verbandsklagerechts. Eine solche Befugnis soll es den Verbänden ermöglichen, im Namen von Betroffenen und im Interesse der Allgemeinheit auch dann gegen Datenschutzverstöße vorzugehen, wenn die Betroffenen keine rechtlichen Schritte gegen den Rechtsverletzer einleiten.

Technischer Datenschutz

Die Enquete-Kommission hat in ihrem Bericht festgestellt, dass die aktuellen Rechtsnormen oft nicht mehr geeignet sind, Datensicherheit und Datenschutz zu gewährleisten, weil sie weder zeitgemäß sind noch technikneutral formuliert sind. Sie hat auch festgehalten, dass eine technikneutrale Formulierung zum Beispiel anhand von Schutzzielen – wie dies die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt – geeignet sein kann, gesetzliche Normen trotz der ständigen technischen Weiterentwicklung beständiger zu gestalten.

Deshalb wird dem Deutschen Bundestag empfohlen,

die technischen und organisatorischen Maßnahmen (im Sinne der Anlage zu § 9 BDSG) zu reformieren, indem die Definitionen der elementaren Schutzziele aufgenommen werden, so dass sich daraus einfache, flexible und praxistaugliche Maßnahmen ableiten lassen.

Bei der Definition der Schutzziele sollten folgende Punkte beachtet werden:

– Die Schutzziele sollten einfach, verständlich, praxistauglich und technologieunabhängig formuliert sein,

– Maßgabe bei der Definition sollten in erster Linie die Vorgaben des Datenschutzes sein, nicht Vorgaben zur IT-Sicherheit,

– Die Umsetzung muss frühzeitig ansetzen und durch entsprechende Maßnahmen (wie etwa Risikoanalysen und Sicherheitskonzepte, die vor Freigabe des Verfahrens vorgelegt und fortgeschrieben werden müssen) abgesichert werden.

Datenschutz für Kinder und Jugendliche[348]

Es ist festzustellen, dass es verschiedene schutzwürdige Gruppen im Bereich des Datenschutzes gibt. Dabei ist besonders die Gruppe der Kinder und Jugendlichen hervorzuheben, weil sie aufgrund ihrer (noch) nicht ausreichenden Einsichtsfähigkeit in der digitalen Informationsgesellschaft besonders schutzwürdig sind.

Deshalb wird dem Deutschen Bundestag empfohlen,

1. mit klaren gesetzlichen Regelungen festzulegen, ab wann und unter welchen Voraussetzungen Minderjährige eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können,

2. allgemein gesetzlich festzulegen, dass bei Angeboten für Kinder und Jugendliche die Erhebung von personenbezogenen Daten auf das erforderliche Mindestmaß für die Dienstleistung beschränkt bleiben muss. Zuwiderhandlungen beziehungsweise Verstöße müssen besonders stark sanktioniert werden,

3. zu prüfen, inwieweit darüber hinaus spezielle Datenschutzregelungen für Kinder und Jugendliche getroffen werden müssen, zum Beispiel im Hinblick auf den Bereich der sozialen Netzwerke oder bei Kaufangeboten wie Onlinespielen, Klingeltönen etc.,

4. Anbieter von Onlinediensten, die von Kindern und Jugendlichen genutzt werden, zu verpflichten, die Hinweise zum Datenschutz so verständlich zu machen, dass Kinder und Jugendliche diese auch verstehen. So könnten beispielsweise die AGB und die Datenschutzerklärungen neben den juristisch verbindlichen Textversionen in leicht verständlichen Versionen angeboten werden,

5. auf die Einführung eines allgemein gültigen Datenschutzgütesiegels hinzuwirken, speziell zur Orientierung für Kinder und Jugendliche, wie es der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bereits gefordert hat. Dies könnte zum Beispiel durch die Stiftung Datenschutz vergeben werden,

6. sich für eine Stärkung der Medienkompetenz durch Bildungsangebote, etwa der Stiftung Datenschutz, einzusetzen. Es ist notwendig, das Bewusstsein für den Schutz eigener und fremder Daten bei Kindern und Jugendlichen zu entwickeln und zu fördern,

7. Anbieter von Internetdiensten zu verpflichten, etwaige Persönlichkeitsprofile zu löschen und die über die Kinder bekannten Informationen umgehend zu anonymisieren, sobald diesen Anbietern das Alter eines minderjährigen Kindes bekannt wird,

8. Anbietern von Internetdiensten die Weitergabe und den Weiterverkauf von Daten von Kindern und Jugendlichen sowie Profilen von minderjährigen Nutzerinnen und Nutzern zu untersagen,

9. die Erhebung und Erstellung von Persönlichkeits-, Konsum- und Vorliebenprofilen von minderjährigen Nutzerinnen und Nutzern grundsätzlich zu untersagen.

Hinsichtlich weiterer entsprechender Handlungsempfehlungen wird auf den Zwischenbericht Medienkompetenz der Enquete-Kommission[349] verwiesen.

Profilbildung[350]

Die Enquete-Kommission stellt in ihrem Bericht fest, dass die Zusammenführung und Verknüpfung personen-

[348] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[349] Bundestagsdrucksache 17/7286 vom 21. Oktober 2011, online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Medienkompetenz_1707286.pdf

[350] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

bezogener Daten zu Profilen (wie zum Beispiel durch das so genannte Behavioral Targeting) eine besondere Gefahr für das Persönlichkeitsrecht darstellen kann. Durch solche Techniken können das Verhalten, die Interessen und die Gewohnheiten eines Menschen vorhersehbar gemacht werden, was nicht zuletzt eine gezielte Manipulation ermöglicht, unabhängig davon, ob dies zu Werbe- oder sonstigen Zwecken erfolgt.

Aufgrund des Gefährdungspotentials wird dem Deutschen Bundestag empfohlen,

1. die Schaffung einer gesetzlichen Definition der Profilbildung und deren grundsätzliches, gesetzlich verankertes Verbot mit einem allgemeinen Ermächtigungsvorbehalt sowie die Schaffung von gesetzlichen Ausnahmen, die nur zulässig sind, wenn sie dem besonderen Gefährdungspotential Rechnung tragen oder durch freiwillige, aktive und informierte Einwilligung der Betroffenen legitimiert sind. Diese Einwilligung setzt eine umfassende Information über Umfang und Herkunft der verwandten Daten, Zweck und Verwendung des Profils, die verantwortliche Stelle und die vorgesehene Löschungsfrist voraus. Die Einwilligung muss freiwillig und jederzeit widerrufbar sein. Der Widerruf muss die sofortige Löschung des Profils zur Folge haben, auch bei den Stellen, an die es übermittelt worden ist,

2. angesichts des umfassenden und weit verbreiteten Einsatzes von Instrumenten zum Zwecke des Behavioral Targeting Initiativen zu unterstützen, die eine anbieterunabhängige, aktive Information der Öffentlichkeit über Funktionsweisen, eingesetzte Techniken, mögliche Schutzmechanismen sowie die derzeitigen rechtlichen Regelungen zum Inhalt haben,

3. die Webseitenbetreiber ebenso wie Werbewirtschaftsunternehmen zu verpflichten, verständlich und leicht einsehbar über die konkret eingesetzten Analysetechniken zu informieren und die Möglichkeit einer begrenzten Einwilligung aufzuzeigen.

Veröffentlichung von Daten im Internet

Mit der Verbreitung so genannter Web 2.0 Anwendungen wird die Veröffentlichung von personenbeziehbaren Informationen insbesondere durch andere Privatpersonen im Rahmen der Nutzung zum Beispiel von sozialen Netzwerken möglich. Mit dem Wegfall technischer Grenzen der Publizierbarkeit häufen sich Konflikte um Veröffentlichungen, die gegen Persönlichkeitsrechte verstoßen können oder von den Betroffenen aus anderen Gründen abgelehnt werden.

Dem Deutschen Bundestag wird empfohlen,

zu prüfen, ob durch ein allgemeines, auch gegenüber den Internetanbietern geltend zu machendes Widerspruchsrecht gegen personenbezogene Internetveröffentlichungen ein wesentlich verbesserter Schutz des Persönlichkeitsrechts der Betroffenen bewirkt werden kann.

Cloud-Computing[351]

Es ist festzustellen, dass das Cloud-Computing zukünftig eine große Herausforderung für den Datenschutz darstellt. Deshalb ist es unerlässlich, dass sich die Bundesregierung auf internationaler und europäischer Ebene dafür einsetzt, Vereinbarungen und Standards zu erreichen, die einem hohen – möglichst deutschen beziehungsweise europäischen – Schutzniveau entsprechen.

Darüber hinaus wird dem Deutschen Bundestag empfohlen,

1. gesetzliche Regelungen zu schaffen, die datenschutzrechtliche Mindeststandards dafür festlegen, unter welchen Umständen personenbezogene beziehungsweise personenbeziehbare Daten ausgelagert werden dürfen. Die Nichteinhaltung dieser Mindeststandards muss sanktioniert werden,

2. weitere gesetzliche Regelungen zu schaffen, die Verantwortlichkeiten und entsprechende Dokumentationspflichten über die Auslagerung beziehungsweise Weitergabe von Daten klar regeln

3. die Anbieter von Clouds zu verpflichten, Art und Ort der Datenverarbeitung offenzulegen sowie Angaben zu den Sicherungsmaßnahmen zu machen,

4. eine gesetzliche Regelung zu schaffen, die sicherstellt, dass personenbezogene Daten nur auf deutschen beziehungsweise europäischen Servern gespeichert werden dürfen, bei denen ein entsprechendes Datenschutzniveau sichergestellt ist.

Regulierte Selbstregulierung und Auditierung

Es ist festzustellen, dass eine Selbstregulierung im Datenschutz eine wertvolle Ergänzung zu den gesetzlichen Regelungen darstellen kann, weil sie den gerade für den Internetbereich wichtigen Vorzug der Flexibilität und Anpassung an neue Gegebenheiten besitzt. Ein hohes Schutzniveau wird jedoch nur erreichbar sein, wenn die Selbstregulierung in einen gesetzlichen Rahmen eingebunden ist, es sich also der Sache nach um eine Koregulierung handelt. Ein Beispiel bietet § 38a BDSG, der aber bislang mangels Akzeptanz in der Privatwirtschaft noch nicht die beabsichtigte Wirkung entfalten konnte. Reine Selbstregulierungen bleiben sinnvoll und notwendig, wenn es sich unterhalb der gesetzlichen Regelungsziele um freiwillige zusätzliche Bemühungen der Wirtschaft handelt.

Darüber hinaus ist festzustellen, dass Datenschutzaudits und Datenschutzgütesiegel ein wesentliches Instrument zur Vertrauensbildung im gegenseitigen Verhältnis von Bürgern, Unternehmen und Staat darstellen können.

Deshalb wird dem Deutschen Bundestag empfohlen,

1. zu prüfen, wie die Integration von selbstregulativen Elementen in das Konzept des Bundesdatenschutzge-

351 Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

setzes verbessert werden kann, ohne das Schutzniveau zu senken. Mit § 38a BDSG existiert zwar eine Norm mit explizit selbstregulativen Elementen, die sogar im Grundsatz sowohl von den Unternehmen als auch von den Datenschutzbeauftragten begrüßt wird, jedoch in der Praxis kaum angewandt wird. Es steht zu vermuten, dass dies an den nicht hinreichend konkret ausgestalteten Verfahren liegt,

2. ein Datenschutzauditgesetz gemäß § 9a BDSG zu verabschieden, welches den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bietet und dessen Verfahren unbürokratisch, aber verbindlich ausgestaltet sein muss,

3. im Rahmen von Vergabegesetzen eine Verpflichtung öffentlicher Stellen zu verankern, solche auditierten beziehungsweise zertifizierten Produkte bevorzugt einzusetzen. Soweit keine Vergabegesetze bestehen, ist im Rahmen der Ausschreibungen zu berücksichtigen, dass besonders datenschutzfreundliche Produkte bevorzugt eingekauft oder genutzt werden.

Stiftung Datenschutz[352]

Es ist festzustellen, dass die geplante Stiftung Datenschutz, wenn die richtigen Vorgaben für die inhaltliche Ausgestaltung gefunden werden, als wirkungsvolle Plattform vorhandene Angebote zusammenführen und so ihrem geplanten Auftrag für Aufklärung und Information gerecht werden kann. Die von der Bundesregierung auf den Weg gebrachte Stiftung Datenschutz ist daher im Grundsatz zu begrüßen. Diese Stiftung kann unter anderem Kriterien für die Zertifizierung von Diensten sowie für ein einheitliches Gütesiegel aufstellen und damit mehr Transparenz für Unternehmen und Bürger erwirken. Dadurch kann sich auch eine Erleichterung bei der Auswahl zwischen einer Vielzahl von Anbietern ergeben und zugleich das Vertrauen der Bürgerinnen und Bürger in neue Technologien gestärkt werden. Für Unternehmen kann sie Anreize setzen, hohe datenschutzrechtliche Anforderungen einzuhalten. Neben der Festlegung von Kriterien nimmt sie die Vergabe von Gütesiegeln nach einem gesetzlich geregelten Verfahren vor.

Bei der Einrichtung der Stiftung Datenschutz ist darauf zu achten, dass vergleichende Tests nach verschiedenen Kriterien, unter Einschluss des Datenschutzes, bereits etwa durch die Stiftung Warentest durchgeführt werden; und zwar für Güter, Produkte und Dienstleistungen, die sich explizit an Endverbraucher richten. Eine klare Zuordnung der Zuständigkeit in diesem Bereich ist deshalb in der Satzung zu verankern. Eine Überschneidung der Zuständigkeiten zwischen den beiden Stiftungen sollte vermieden werden. Vielmehr sollen diese sich in ihren Angeboten ergänzen.

Weitere Aufgaben können die Stärkung des Selbstdatenschutzes sowie Aufklärung und Bildung im Datenschutz sein.

[352] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

Die Bundesregierung wird daher aufgefordert, bei Einsetzung der Stiftung folgende Punkte – die für eine wirkungsvolle Arbeit einer Bundesstiftung Datenschutz mit vorstehendem Auftrag unabdinglich sind – zu berücksichtigen:

1. Die Stiftung ist wirtschaftlich und organisatorisch, also finanziell und personell, unabhängig von den zu bewertenden Unternehmen zu organisieren. Personell ist darauf zu achten, dass bei der Besetzung der Gremien die zu prüfenden datenverarbeitenden Unternehmen zwar beteiligt werden, aber auf die Unabhängigkeit der Stiftung keinen Einfluss haben. Dies könnte zum Beispiel durch die Einsetzung eines Beirats, der beratende Funktion hat, geschehen. Finanziell sollte die Bundesstiftung nicht allein vom Bundeshaushalt abhängig sein. Bei der Annahme von Zuwendungen hat die Stiftung jedoch darauf zu achten, dass ihre Unabhängigkeit gewahrt bleibt.

2. In der Satzung ist das Verhältnis zu den Datenschutzbehörden zu klären. Es ist festzuhalten, dass diesen allein die Kontrolle über die Einhaltung der Gesetze obliegt und die Aufsichtstätigkeit nicht durch die Arbeit der Stiftung beeinflusst werden darf. Ebenso dürfen die von der Stiftung Datenschutz erteilten Audits und Gütesiegel keine rechtliche Bindungswirkung gegenüber den Datenschutzbehörden entfalten, das heißt die Aufsichtsbehörden müssen die entsprechenden Unternehmen dennoch anlassbezogen überprüfen dürfen.

3. Es ist in der Satzung zu regeln, wer die materiellen Standards für Zertifizierungsverfahren setzt. Dabei sind ein Höchstmaß an Transparenz sowie eine enge Kooperation mit den Datenschutzbehörden unabdingbar.

4. Die Vergabe von Audits kann durch die Stiftung Datenschutz aufgrund eines bundeseinheitlich gesetzlich festgelegten Auditierungsverfahrens erfolgen. Hierfür bedarf es eines Gesetzes im Sinne von § 9a BDSG. Dabei ist zu beachten, dass bereits existierende Auditverfahren (wie zum Beispiel in Bremen oder Schleswig-Holstein) in die Ausgestaltung und Vergabe eingebunden werden.

5. Bei der Vergabe von Gütesiegeln durch die Stiftung ist darauf zu achten, dass ein einheitliches Gütesiegel entwickelt wird und eine inflationäre Handhabung bei der Vergabe vermieden wird. Ebenso ist das Verfahren für die Vergabe transparent zu gestalten. Die Gütesiegel sind nur für eine bestimmte Zeit (zum Beispiel für zwei Jahre) zu erteilen und müssen turnusgemäß geprüft werden.

6. Im Bereich der Bildung darf die Stiftung Datenschutz nicht die Zuständigkeit der Länder verletzen. Die Länder sind deshalb mitentscheidend einzubeziehen. Schwerpunkt der Stiftungstätigkeit sollte deshalb die außerschulische Bildung sein.

7. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Informationsportal oder ein virtuel-

les Datenschutzbüro (wie derzeit beim ULD Schleswig-Holstein[353] praktiziert) zu schaffen.

8. Die Stiftung Datenschutz sollte perspektivisch auch im Bereich der Datenschutzforschung, insbesondere der Entwicklung und dem Ausbau von Instrumenten des technischen Datenschutzes, tätig werden. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der Koordination der Forschungsmittelvergabe als auch für den Bereich eigener Forschungsanstrengungen.

Schadensersatzansprüche[354]

Im Ergebnis ist festzustellen, dass Handlungsbedarf im Bereich des Schadensersatzrechts besteht.

Deshalb wird dem Deutschen Bundestag empfohlen,

1. bezugnehmend auf die Vorschläge der Konferenz des Bundes- und der Landesdatenschutzbeauftragten eine Gefährdungshaftung auch gegenüber nicht-öffentlichen Stellen einzuführen,

2. einen pauschalierten Schadensersatzanspruch bei Datenschutzverstößen einzuführen, der die Problematik der Bezifferbarkeit des Schadens löst und alle datenverarbeitenden Stellen zum Ersatz immaterieller Schäden verpflichtet, unabhängig von nachweisbaren weiteren und höheren Schäden,

3. zu prüfen, ob nicht die Festlegung einer Mindest- und einer Höchstgrenze der Ersatzsumme erfolgen sollte.

Beschäftigtendatenschutz[355]

Es ist festzustellen, dass es im Bereich des Datenschutzes für Beschäftigte gesetzgeberischen Handlungsbedarf gibt. Hierbei sind insbesondere die Rechte der Beschäftigten bei Überwachung und Screening zu wahren.

Dem Deutschen Bundestag wird deshalb empfohlen, ein entsprechendes Gesetz unter Beachtung nachfolgender Kriterien zu beschließen:

1. Der Beschäftigtendatenschutz ist in einem eigenständigen Gesetz zu regeln. Die derzeit bestehenden Regelungen im Bundesdatenschutzgesetz sind nicht effektiv genug. Denn es finden die allgemeinen Regelungen des Datenschutzes auch auf das Beschäftigungsverhältnis Anwendung. Diese sind oft nicht explizit auf den Persönlichkeitsrechtsschutz der Beschäftigten zugeschnitten.

2. Eine eigenständige gesetzliche Regelung muss die dem Arbeitsverhältnis immanente Abhängigkeit der Beschäftigten vom Arbeitgeber aufgreifen und eine Generaleinwilligung für die Datenerhebung und -nutzung schon bei Aufnahme des Arbeitsverhältnisses, aber auch während des Arbeitsverhältnisses verhindern.

3. Das Gesetz muss die anlasslose Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz, aber auch im privaten Umfeld verbieten. Dieses grundsätzliche Verbot muss die direkte Überwachung durch Beauftragte, Externe oder Mitarbeiter, aber auch die indirekte Überwachung durch Video- oder Tonaufnahmen umfassen. Auch biometrische oder ferngesteuerte Systeme (RFID, GPS oder Fernwartungssoftware auf Mitarbeiter-PCs) dürfen nicht über eng begrenzte Zwecke hinaus eingesetzt werden und bedürfen der Vorabkontrolle.

4. Bei der Nutzung von Internet und E-Mail ist dem Persönlichkeitsrecht der Beschäftigten in besonders hohem Maße Rechnung zu tragen. Es muss ein grundsätzliches Verbot des Zugriffs auf personenbezogene oder -beziehbare Nutzerdaten bei der Verwendung dieser modernen Kommunikationsmittel festgelegt werden. Dieses Verbot darf nicht durch eine Generaleinwilligung der Beschäftigten – etwa mit Abschluss des Arbeitsvertrages – ausgeschlossen werden.

5. Ausgehend von dem Grundsatz, dass der Zweck des Datenschutzes darin besteht, die Einzelnen vor Missbrauch ihrer Daten zu schützen, können Ausnahmen nur für gesetzlich ausdrücklich geregelte Fälle vorgesehen werden. Dies ist insbesondere nur dann zuzulassen, wenn eine andere Aufklärung, namentlich durch die Polizei oder die Staatsanwaltschaft, nicht möglich ist. Ausnahmen sind für Fälle des begründeten Verdachts einer Straftat oder der schwerwiegenden Schädigung des Arbeitgebers zuzulassen. Hierzu sind das Zustimmungserfordernis der Interessenvertretung oder, sofern nicht vorhanden, die Einbeziehung einer neutralen Stelle (zum Beispiel des Landesdatenschutzbeauftragten) erforderlich.[356]

6. Es ist notwendig, das Fragerecht des Arbeitgebers bei der Einstellung und die Möglichkeit der Anordnung von ärztlichen Untersuchungen im Gesetz auf die durch die Rechtsprechung beurteilten Fälle zu beschränken. Die Anordnung von ärztlichen Untersuchungen bedarf der Zustimmung des Betriebsrates.

7. Vor der Erhebung von Beschäftigtendaten im Rahmen eines Einstellungsverfahrens ist über die Art der auszuübenden Tätigkeit und deren Einordnung in den Arbeitsablauf des Betriebs zu unterrichten.

8. Es bedarf einer Sonderregelung im Gesetz für den folgenden Fall: Sind Beschäftigte auch Kunden ihres Arbeitgebers, müssen die Daten des Kundenbereichs gesondert geführt und geschützt werden. Personalverantwortliche dürfen keinen Zugriff auf diese Kundendaten haben.

---

[353] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

[354] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[355] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[356] Siehe hierzu: Däubler, Wolfgang u. a.(Hrsg.): Bundesdatenschutzgesetz. 2010, S. 558 ff.

9. Fälle des so genannten Whistleblowings sind gesetzlich gesondert zu verankern und mit einem Maßregelungsverbot zu versehen.[357]

10. Ein eigenständiges Beschäftigtendatenschutzgesetz muss die Rechtsposition des betrieblichen Datenschutzbeauftragten stärken, so zum Beispiel durch eine weiter verbesserte Kündigungsschutzregelung.

11. Die Mitbestimmungsrechte der Betriebsräte beim Datenschutz sind durch das Gesetz zu stärken.

12. Für die Daten von Mitgliedern des Betriebsrats und von Aufsichtsräten ist ein Immunitätsschutz für die Dauer ihrer Amtszeit zu prüfen beziehungsweise darüber hinaus in Anlehnung an die Vorschriften zum Sonderkündigungsschutz, die im Kündigungsschutzgesetz gelten.

13. Um die von Datenschutzverstößen betroffenen Beschäftigten in der Rechtsdurchsetzung zu stärken, muss das Gesetz eine Verbandsklagemöglichkeit vorsehen. Denn im bestehenden Arbeitsverhältnis wird eine Klage gegen den Arbeitgeber erfahrungsgemäß nicht angestrengt. Hierzu ist die Gefahr von Repressalien zu groß.

14. In einem Beschäftigtendatenschutzgesetz ist ein konkreter Anspruch auf Schmerzensgeld für den in seinem Persönlichkeitsrecht verletzten Beschäftigten (zum Beispiel entsprechend § 15 Allgemeines Gleichbehandlungsgesetz[358]) zu verankern.

15. In dem Gesetz müssen die Ansprüche der Beschäftigten bei Verstößen gegen den Beschäftigtendatenschutz konkret, klar und verständlich geregelt werden. Es bedarf unter anderem eines Unterlassungsanspruchs gegenüber dem Arbeitgeber sowie eines Schadensersatzanspruchs für Vermögensschäden und immaterielle Schäden.

Ubiquitous Computing

Nach den Datenschutzkonzepten der 1960er und 1970er Jahre, denen die damalige Großrechnertechnologie zugrunde lag, bedarf es jetzt schlüssiger Antworten auf die weltweite Vernetzung von Rechnern in einem eigenen „virtuellen Sozialraum“ des Internets. Gleichzeitig beginnt mit der vernetzten Digitalisierung von Infrastrukturen (zum Beispiel im Bereich Verkehr oder bei Stromnetzen) und Alltagsgegenständen unter anderem mit Sensoren wie den RFID (etwa des so genannten intelligenten Kühlschrankes) bereits die nächste große Herausforderung, auf die es noch keine regulatorische Antwort gibt. Kennzeichen dieser unter dem Stichwort Ubiquitous Computing zusammengefassten Entwicklung ist die (oft ad hoc erfolgende) Verknüpfung der körperlichen Alltagswelt mit der virtuellen Welt des Internets. Die mit Sensortechnik ausgestatteten Alltagsgegenstände nehmen Veränderungen ihrer Umwelt wahr, vernetzen sich mit vergleichbaren Gegenständen und reagieren kontextbezogen. Über die Verbindung mit den Besitzern der Gegenstände erfolgen zumindest mittelbar umfangreiche Speicherungen personenbeziehbarer Daten auf Vorrat sowie Nutzerprofile. In der Summe können auf diese Weise verhältnismäßig dichte Überwachungsnetze hinsichtlich der sich in diesen interaktiven Umgebungen bewegenden Personen entstehen. Mit den bisherigen Grundprinzipien des Datenschutzes sind diese Anwendungen kaum in Einklang zu bringen.[359]

Dem Deutschen Bundestag wird im Hinblick auf die Entwicklungen der allgegenwärtigen Datenverarbeitung empfohlen,

1. die beginnende tatsächliche Ausbreitung von Anwendungen des Ubiquitous Computing ständig sorgsam zu beobachten,

2. der Grundsatz verpflichtender technischer Vorkehrungen (Privacy by Design) bei der Entwicklung und dem Einsatz von Produkten des Ubiqitous Computing muss mit Blick auf die Funktionsweise und die besonderen Risiken gegebenenfalls gesetzlich konkretisiert werden,

3. Einschränkungen, die sich hinsichtlich der Anwendbarkeit zentraler Grundsätze des bisherigen Datenschutzrechts ergeben, durch angemessene, ein vergleichbar hohes Schutzniveau gewährleistende anderweitige Vorgaben zu kompensieren,

4. dafür Sorge zu tragen, dass die eingesetzten Technologien zugleich für Nutzerinnen und Nutzer die Möglichkeit einer kontinuierlichen Erläuterung und Abrufbarkeit ihres Status – mit Blick auf zum Beispiel Profilbildung oder Vernetzungsgrad mit anderen Anwendungen – gewährleisten, da der Grundsatz der Transparenz angesichts der weitgehend im Hintergrund stattfindenden vielfältigen Datenverarbeitungen besondere Bedeutung gewinnt.

Geolocation/Geodaten

Es ist festzustellen, dass sich mit der digitalen Gesellschaft zunehmend auch eine digitale Öffentlichkeit herausbilden wird. Zu dieser digitalen Öffentlichkeit gehört auch das Angebot und die Nutzung von Geoinformationen beziehungsweise Geodiensten und -anwendungen im Internet, zum Beispiel Kartierungs- und Lokalisierungsdienste wie Google-Street-View, Microsoft Streetside, Facebook-Places oder Qype.

Wie in der analogen Welt gilt es, die Öffentlichkeit und den öffentlichen Raum als eine Grundvoraussetzung einer demokratisch verfassten offenen Gesellschaft zu erhalten und gleichzeitig die Privatheit zu schützen. Das bedeutet

[357] Ausführlich zur Thematik des Whistleblowings: Tinnefeld, Marie-Theres/Rauhofer, Judith: Whistleblower: Verantwortungsbewusste Mitarbeiter oder Denunzianten? DuD 2008, 717 ff.

[358] Allgemeines Gleichbehandlungsgesetz vom 14. August 2006, BGBl. I, S. 1897, zuletzt geändert durch Artikel 15 Absatz 66 des Gesetzes vom 5. Februar 2009, BGBl. I, S. 160.

[359] Vgl. dazu insgesamt Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. MMR 2005, 71 ff.

auch, die grundrechtlich abgesicherten Positionen wie Wissenschafts-, Presse- und unternehmerische Freiheit mit anderen Grundrechten wie dem Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen. Es ist festzuhalten, dass Selbstverpflichtungen der in diesem Bereich tätigen Unternehmen hilfreiche Instrumente darstellen. Wenn Persönlichkeitsrechte betroffen sind, bedürfen sie aber jedenfalls eines gesetzlichen Rahmens.

Unter Bezugnahme auf die Forderungen der Datenschutzbeauftragten des Bundes sowie der Länder wird dem Deutschen Bundestag empfohlen, eine allgemeine, technikunabhängige Regelung zur Verarbeitung von personenbezogenen Geoinformationen beziehungsweise -daten zu schaffen, die sich an den jeweiligen Risiken orientiert. Hierbei sollten folgende Gesichtspunkte beachtet werden:

1. Es sollten Kriterien geschaffen werden, die festlegen, über welche Verfahren eine Interessenabwägung zwischen Persönlichkeitsschutz und Informationsinteresse vorgenommen werden kann, und wonach eine klare Abgrenzung zwischen reinem Sachbezug und Personenbeziehbarkeit möglich ist.

2. Es sollte eine gesetzliche Verpflichtung geschaffen werden, wonach den Betroffenen die Tatsache der konkreten Ortung in verständlicher Form anzuzeigen ist, zum Beispiel durch ein akustisches Signal, sobald die oder der Betroffene geortet wurde.

3. Weiterhin ist eine Regelung zu treffen, wonach der Einsatz von Tracking-Systemen, also jede Form der Ortung durch Dritte, die der Betroffene nicht beeinflussen kann, nur mit dessen Einwilligung (nach dem Vorbild von § 98 TKG) zulässig ist.

4. Unternehmen, die grundsätzlich sachbezogene, aber personenbeziehbare Geoinformationen, welche schutzwürdige entgegenstehende Interessen der Betroffenen berühren können, im Internet zur Nutzung oder zur Verarbeitung veröffentlichen, müssen diesen (zum Beispiel Eigentümern oder Mietern) ein Widerspruchsrecht anbieten. Das entsprechende Recht muss gesetzlich festgeschrieben und kann nicht allein durch eine Selbstverpflichtung der anbietenden Unternehmen geregelt werden.

5. Verstöße gegen entsprechende Regelungen müssen sanktioniert werden, wobei die Aufsicht hierüber den Datenschutzbeauftragten des Bundes und der Länder sowie den Aufsichtsbehörden über den Datenschutz im nicht-öffentlichen Bereich obliegen sollte.

Videoüberwachung[360]

Der Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen breitet sich weiterhin aus. Damit verbunden sind massenhafte Bilderfassungen und Bildspeicherungen von völlig unbeteiligten Personen. Die tatsächlichen Einsatzbedingungen, beispielsweise die Frage des konkreten Zwecks, technische Möglichkeiten wie etwa das Zoomen oder die Frage, ob es sich um eine internetgestützte Bildübertragung handelt, bleiben für die Betroffenen weithin intransparent. Darüber hinaus fehlt es an einer hinreichenden und aktuellen Übersicht, in welchem Umfang vor allem städtische Räume bereits von Videoüberwachungen betroffen sind. Die Datenschutzbeauftragten der Länder haben in den vergangenen Jahren auf zahlreiche weitere Probleme des zunehmenden Kameraeinsatzes aufmerksam gemacht, darunter insbesondere das gewaltige Vollzugsdefizit hinsichtlich der Beachtung der gesetzlichen Vorschriften. Die bestehenden gesetzlichen Regelungen, insbesondere § 6b BDSG, haben auch inhaltlich keine Einschränkung dieser Entwicklung bewirken können und bieten den Bürgern nur unzureichenden rechtlichen Schutz.

Deshalb wird dem Deutschen Bundestag empfohlen,

1. im Rahmen einer Reform insbesondere des Bundesdatenschutzgesetzes die Zulässigkeit der Bilderfassung öffentlich zugänglicher Räume enger zu begrenzen,

2. sachgerechte Regelungen für eine verbesserte Transparenz und Sicherheit beim Einsatz von Videotechnik auf den Weg zu bringen, darunter auch Maßnahmen zur laufenden Beobachtung und Erfassung der Ausbreitung,

3. die Bundesregierung anzuhalten, im Rahmen der Erneuerung der Datenschutzrichtlinie auf zulässigkeitsbegrenzende Bestimmungen für den Einsatz von Videoüberwachungen zu drängen.

Datenschutz auf technischer Ebene (Deep Packet Inspection und IPv6)[361]

Der Datenverkehr von Nutzern im Internet sollte einem vollständigen Telekommunikationsgeheimnis unterliegen. Die Kommunikation von Bürgerinnen und Bürgern untereinander, mit staatlichen Stellen oder mit privaten Unternehmen gehört, wenn sie nicht von den Betroffenen selbst öffentlich gemacht wird, zur schützenswerten Privatsphäre jedes Einzelnen. Netzwerkmanagementmaßnahmen, etwa mit Hilfe von so genannter Deep Packet Inspection (DPI), bei der die von Teilnehmern gesendeten und empfangenen Inhalte durchleuchtet beziehungsweise auch auf der Inhaltsebene ausgelesen und analysiert werden, sind unter diesem Gesichtspunkt abzulehnen.

Durch die rasant ansteigende Zahl von Geräten, die mit dem Internet verbunden sind beziehungsweise darüber kommunizieren, ist bereits seit geraumer Zeit klar, dass der verwendbare Adressraum des IPv4-Protokolls ausgeschöpft und nicht zukunftsfähig ist. Die anstehende Einführung des IPv6-Protokolls in den Internetalltag bietet den Vorteil einer ungleich größeren Anzahl möglicher IP-Adressen im Internet. Mit Nutzung von IPv6 ist es daher technisch möglich jedem internetfähigen Endgerät eine

---

[360] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[361] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

dauerhafte, nur einmal vergebene IP-Adresse zuzuweisen. Somit ist die Kommunikation eines einzelnen Endgerätes theoretisch über Jahre hinweg nachvollziehbar.

Dem Deutschen Bundestag wird empfohlen,

1. die Verwendung von Methoden zur inhaltlichen Analyse von (IP-)Datenpaketen (zum Beispiel DPI) beziehungsweise die Analyse selbst zu untersagen. Dies gilt für Eingriffe von staatlicher und nicht staatlicher Seite gleichermaßen und muss technikneutral formuliert werden,

2. Internet-Zugangsanbieter zu verpflichten, ihren Kunden ohne Mehrkosten die Auswahl zwischen dauerhaft festen und wechselnden IP-Adressen für ihre Anschlüsse beziehungsweise Endgeräte anzubieten[362].

Sicherheitsbehörden und die Evaluierung von Eingriffsbefugnissen[363]

Dem Deutschen Bundestag wird empfohlen, die bestehenden Aufgaben und Befugnisse von Sicherheitsbehörden und Diensten, die mit Grundrechtseingriffen verbunden sind, umfassend hinsichtlich ihrer Notwendigkeit, Wirksamkeit und Effizienz sowie ihrer grundrechtswahrenden Funktion unabhängig, auf wissenschaftlicher Grundlage und ergebnisoffen zu evaluieren. Dies betrifft insbesondere die verdeckten Ermittlungsmaßnahmen. Zwar bestehen in zahlreichen Gesetzen bereits Evaluierungsvorschriften, die jedoch in der Umsetzung diesen Ansprüchen zumeist nicht genügen.[364]

4.2.3 Ergänzendes Sondervotum der Fraktion SPD sowie der Sachverständigen Alvar Freude, Lothar Schröder und Dr. Wolfgang Schulz zu Kapitel 3[365]

Vorratsdatenspeicherung

Der grundrechtliche Schutz informationeller Selbstbestimmung wurde durch die Rechtsprechung des Bundesverfassungsgerichts in jüngerer Zeit schärfer konturiert, nicht zuletzt durch die Entscheidung zur Vorratsdatenspeicherung. Das Bundesverfassungsgericht hat am 2. März 2010[366] entschieden, dass die Vorratsdatenspeicherung in Deutschland in ihrer bisherigen Umsetzung verfassungswidrig sei, da das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzerinnen und Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe, und hat zudem die Hürden für den Abruf dieser Daten als zu niedrig bewertet. Das Urteil verpflichtete deutsche Telekommunikationsanbieter zur sofortigen Löschung der bis dahin gesammelten Daten. Das Bundesverfassungsgericht hat jedoch auch festgestellt, dass die Vorratsdatenspeicherung unter schärferen Sicherheits- und Transparenzvorkehrungen sowie begrenzten Abrufmöglichkeiten für die Sicherheitsbehörden grundsätzlich zulässig sei.

Dem Deutschen Bundestag wird empfohlen,

– eine grundsätzliche und offene Debatte über die Notwendigkeit und auch die Grenzen der Vorratsdatenspeicherung zu führen. Dabei ist auch zu klären, ob und wie eine Speicherung auf Vorrat grundrechtsschonend und verfassungskonform ausgestaltet werden könnte. Eine Zustimmung des Deutschen Bundestages für die Vorratsdatenspeicherung kann es nur geben, wenn es zu einer grundsätzlichen Überarbeitung der damaligen Vorgaben zur Umsetzung der Vorratsdatenspeicherung und auch der europäischen Rechtsgrundlage kommt,

– auch mögliche Alternativen zu einer anlasslosen Vorratsdatenspeicherung zu prüfen,

– zu klären, ob bezüglich der Dauer einer Speicherung und des Datenumfangs eine Rückkehr zu der bis circa 2006 geltenden Situation möglich ist: Internet-Access-Provider haben damals IP-Adressen circa 80 Tage gespeichert, E-Mail-Verbindungsdaten hingegen nur wenige Tage zu technischen Analysezwecken,

– dass, sofern eine Datenspeicherung auf Vorrat erfolgen soll, die Art der zu speichernden Daten als auch die Speicherdauer nicht einzelnen Unternehmen überlassen werden darf, sondern gesetzlicher Regelungen bedürfen.

Deshalb wird der Deutsche Bundestag aufgefordert,

1. die Bundesregierung aufzufordern, auf europäischer Ebene darauf hinzuwirken, dass die Vorratsdatenspeicherungsrichtlinie grundlegend überarbeitet und eine Verkürzung der Speicherfrist auf deutlich unter 6 Monaten aufgenommen wird. Dabei sollten insbesondere für sensible Daten wie beispielsweise Telefon-Verbindungsdaten, Mobilfunk-Ortsdaten und E-Mail-Verbindungsdaten maximal eine auf wenige Tage beschränkte Speicherdauer und hohe Zugriffshürden gelten. Bei den weniger sensiblen, aber in der Praxis wichtigeren IP-Adressen sind längere Speicherfristen denkbar,

2. dass, sollte an der Vorratsdatenspeicherung festgehalten werden, verfassungskonforme gesetzliche Regelungen notwendig sind, die eine Speicherung von und den staatlichen Zugriff auf diese Daten regeln und mit dem Urteil des Bundesverfassungsgerichts vereinbar sind.

---

[362] Die Forderung, dass im Hinblick auf die Einführung von IPv6 bei jedem Einwahlvorgang die dynamische Zuteilung einer neuen IP-Adresse anzubieten sei, ist aus der Beteiligungsplattform der Enquete-Kommission übernommen worden.

[363] Die Sachverständige Constanze Kurz schließt sich dieser Handlungsempfehlung an.

[364] Die Handlungsempfehlung „Sicherheitsbehörden und die Evaluierung von Eingriffsbefugnissen“ geht auf den Vorschlag „Systematische Evaluierung aller Überwachungsgesetze“ auf der Beteiligungsplattform der Enquete-Kommission zurück.

[365] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu Kapitel 3 an.

[366] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, NJW 2010, 833 – Vorratsdatenspeicherung.

Bei der konkreten Fassung der Regelungen sollten folgende Anforderungen mit aufgenommen werden:

1. Der Abruf und die Nutzung der Verbindungsdaten darf nur bei Verdacht auf schwerste Straftaten erfolgen. Das sind insbesondere Straftaten gegen das Leben, die körperliche Unversehrtheit und die sexuelle Selbstbestimmung.
2. Als milderes und weniger eingriffsintensives Mittel kann eine Beauskunftung von IP-Adressen geregelt werden. Dabei sollte ein Abruf innerhalb einer kurzen Frist von wenigen Tagen ab Speicherung zudem zum Zwecke der Verfolgung von Straftaten erfolgen können. Nach Ablauf dieser Frist darf der Datenabruf bis zur Löschung der Daten nur noch zur Verfolgung schwerster Straftaten erfolgen.
3. Für Berufsgeheimnisträger ist ein absolutes Verwertungsverbot vorzusehen.
4. Der Abruf aller Verbindungsdaten soll unter Richtervorbehalt stehen.
5. Es ist eine Unterrichtungspflicht für die von einem Datenabruf Betroffenen aufzunehmen. Dies gebietet das Rechtsstaatsverständnis und entspricht im Übrigen den verfassungsrechtlichen Vorgaben.
6. Die Bestimmungen zum technischen Datenschutz müssen entsprechend den verfassungsgerichtlichen Vorgaben deutlich ausgebaut werden. Dazu gehören namentlich eine getrennte Speicherung, die sichere Verschlüsselung von Daten, das Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln und eine revisionssichere Protokollierung von Zugriff und Löschung.
7. Eine effektive Kontrolle muss gewährleistet werden, Verstöße müssen wirksam sanktioniert werden.
8. Eine Nutzung der Daten darf ausschließlich für strafrechtliche, nicht für zivilrechtliche Auskünfte erfolgen.

Eine unterschiedliche Behandlung von IP-Adressen und anderen sensiblen Daten ist bereits im genannten Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung angelegt, ergibt sich aber auch aus der Eingriffstiefe und Sensibilität der Daten. Mit Telefon- und E-Mail-Verbindungsdaten lassen sich umfangreiche Nutzungs- sowie Kommunikationsprofile, mit Mobilfunkdaten zusätzliche Bewegungsprofile erstellen. Die mit dem Grimme Online Award ausgezeichnete[367] Visualisierung von Zeit Online der aufgrund der ehemaligen gesetzlichen Vorgaben gespeicherten Vorratsdaten von Malte Spitz zeigt eindrucksvoll, was eine allgegenwärtige Beobachtung bedeutet.[368]

Eine viel geringere Eingriffstiefe hat jedoch die Speicherung der Zuordnung von IP-Adressen zu Anschlussinhabern bei Internetverbindungen. Anders als vielfach behauptet ist damit keine komplette Überwachung des Surfverhaltens der Nutzerinnen und Nutzer möglich. Im Gegensatz zur Durchführung einer gezielten Telekommunikationsüberwachung kann damit nicht festgestellt werden, welche Webseiten ein Internetnutzer aufgerufen hat. Es ist ausschließlich möglich, im Nachhinein nach einer konkreten Straftat bei Kenntnis der IP-Adresse den Anschlussinhaber herauszufinden. Die Sorge einer Totalüberwachung der Bevölkerung ist daher im Gegensatz zur Speicherung von Handy- und E-Mail-Daten unbegründet.

Bei Straftaten, die mit Hilfe des Internets begangen werden, ist die IP-Adresse oftmals die einzige verwertbare Spur. Daher ist der Wunsch der Ermittlungsbehörden nachvollziehbar, dieses Ermittlungsinstrument nutzen zu können. Dennoch sollten die Transparenzpflichten erhöht und die Speicherfristen auf ein Maß verkürzt werden, das auch vor der Vorratsdatenspeicherung jahrelang üblich war.

In der Bevölkerung besteht die Sorge, dass die Speicherung von IP-Adressen weiter zu Massenabmahnungen bei der Nutzung von Peer-to-Peer-Tauschbörsen führt. Allerdings sind diese Abmahnungen auch ohne Speicherung der IP-Adressen durch Echtzeitabfragen oder entsprechende Speicheranforderungen („Quick Freeze") möglich.

Da mit der skizzierten Regelung sowohl den berechtigten Interessen der Strafverfolgung als auch der Privatsphäre der Bürger Rechnung getragen wird und damit eine grundrechtsschonende Lösung vorliegt, sollte der Deutsche Bundestag auf europäischer Ebene eine entsprechende Initiative empfehlen und in Deutschland auf den Weg bringen.

4.2.4 Ergänzendes Sondervotum der Fraktion DIE LINKE. sowie der Sachverständigen Constanze Kurz und Annette Mühlberg zu Kapitel 3[369]

Vorratsdatenspeicherung

Mit Urteil vom 2. März 2010[370] hat das Bundesverfassungsgericht das deutsche Gesetz zur Vorratsdatenspeicherung nach Beschwerden Tausender Bürgerinnen und Bürger aufgehoben. Die Aufhebung der Vorratsdatenspeicherung durch das Bundesverfassungsgericht ist in der Folge ohne Einfluss auf die Aufklärung von Internetdelikten geblieben. Ob Verbindungsdaten der gesamten Bevölkerung ohne Anlass auf Vorrat gesammelt werden oder ob eine Speicherung nur gezielt im Bedarfsfall erfolgt, hat keinerlei statistisch signifikante Auswirkung auf die registrierte Anzahl von Straftaten oder die Aufklärungsquote. Der Wissenschaftliche Dienst des Deutschen

[367] Zur Begründung der Jury siehe: Grimme Online Award. http://www.grimme-institut.de/html/index.php?id=1345

[368] Vgl. ZEIT ONLINE: Verräterisches Handy. Artikel vom 31. August 2009. http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten und Matzat, Lorenz: Malte Spitz' Vorratsdaten: Der Datensatz unter der Lupe. ZEIT ONLINE vom 24. Februar 2011. http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/

[369] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu Kapitel 3 an.

[370] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 – Vorratsdatenspeicherung.

Bundestages kann in einer Bilanz der europäischen Anwendungen für die Jahre 2005 bis 2010 keine signifikanten Änderungen der Aufklärungsquoten feststellen.[371] Im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments konnte der Vertreter der EU-Kommission am 15. Juni 2011 auf Nachfrage kein Beispiel nennen, bei dem die Vorratsdatenspeicherung für die Aufklärung eines grenzüberschreitenden Delikts eine entscheidende Rolle gespielt hätte.

Gleichwohl plant die Bundesregierung eine Wiedereinführung einer Vorratsdatenspeicherung, wenn auch in eingeschränkter Form, unter anderem mit dem Argument, es ginge um die Umsetzung der europäischen Richtlinie. Die Vorratsdatenspeicherung beschädigt jedoch in eklatanter Weise das Recht auf informationelle Selbstbestimmung, wonach jeder Mensch das Recht haben muss, über seine Daten selbst entscheiden zu können, und damit Herr über seine sozialen, politischen und wissenschaftlichen Kontakte und Verbindungen ist.

Mit der Vorratsdatenspeicherung hätte der Staat durch die komplette Protokollierung des Kommunikationsverhaltens der Bevölkerung Zugriff auf unvorstellbar viele Informationen über seine Bürgerinnen und Bürger. Die anlass- und verdachtslose Vorratsdatenspeicherung ist der sanktionierte Ausdruck eines Generalverdachts gegenüber der gesamten Bevölkerung. Denn auch die Registrierung „nur“ der Verbindungsdaten erlaubt weitgehende Rückschlüsse auf den Inhalt der Kommunikation. Die Vorratsdatenspeicherung ist daher ein nicht zu rechtfertigender unverhältnismäßiger Eingriff in die Bürgerrechte.

Dem Deutschen Bundestag wird daher empfohlen,

– keine weiteren gesetzgeberischen Maßnahmen in Richtung anlassloser und verdachtsunabhängiger Vorratsdatenspeicherung zu ergreifen,

– auf europäischer Ebene nicht nur die Reform der Richtlinie zur Vorratsdatenspeicherung mitzugestalten, sondern den vollständigen Verzicht auf dieses Instrument durchzusetzen.

4.2.5 Ergänzendes Sondervotum der Fraktion BÜNDNIS 90/DIE GRÜNEN zu Kapitel 3[372]

Vorratsdatenspeicherung

Verpflichtende anlasslose Speicherungen personenbezogener Daten auf Vorrat sind mit den datenschutzrechtlichen Grundsätzen von Zweckfestlegung und Erforderlichkeit nicht vereinbar. Sie betreffen eine Vielzahl von völlig unbescholtenen Personen unverhältnismäßig und entfalten damit eine maximale grundrechtsbeeinträchtigende Streubreite. Zudem eröffnen sie eine höchst missbrauchsanfällige Datenquelle und können das Vertrauen in die Nutzung moderner Informations- und Kommunikationssysteme beeinträchtigen. Für den behaupteten Nutzen der Vorratsdatenspeicherung fehlt es, auch angesichts der besonderen Eingriffsschwere, an empirisch überzeugenden Nachweisen.

Verfassungsrechtlich sind sie deshalb als schwerer Grundrechtseingriff unter anderem in das Grundrecht auf informationelle Selbstbestimmung allenfalls in engsten Grenzen zulässig und unterliegen besonders hohen Eingriffsschwellen. Das Bundesverfassungsgericht hat in seinem Urteil vom 2. März 2010[373] zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten zusätzliche Anforderungen festgelegt, die für eine Realisierung von Vorratsdatenspeicherungsvorhaben erhebliche tatsächliche als auch rechtliche Hürden bedeuten.

Mit Blick auf die weiter fortbestehende Verpflichtung zur Umsetzung der Vorratsdatenspeicherungsrichtlinie der Europäischen Union und die anhaltende Diskussion um die Wiedereinführung der Vorratsdatenspeicherung wird dem Deutschen Bundestag empfohlen:

1. Gesetzliche Vorhaben zur anlasslosen verpflichtenden Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten sind abzulehnen.

2. Gesetzliche Vorhaben zu anderweitigen anlasslosen verpflichtenden Vorratsdatenspeicherungen personenbezogener Daten begegnen grundlegenden Bedenken hinsichtlich ihrer verfassungsrechtlichen Zulässigkeit und sind deshalb grundsätzlich zu vermeiden.

5 Bürgerbeteiligung in der Projektgruppe Datenschutz, Persönlichkeitsrechte

Fragen des Datenschutzes und der Persönlichkeitsrechte im Internet betreffen jeden Einzelnen unmittelbar. Auch aus diesem Grund nehmen diese Themen in der öffentlichen Diskussion breiten Raum ein. Die Projektgruppe Datenschutz, Persönlichkeitsrechte war deshalb besonders interessiert daran, die Sichtweise und Ideen der Bürgerinnen und Bürger in ihre Diskussionen einzubeziehen.

5.1 Bürgerbeteiligung im Forum zum Thema Einwilligung

Das Thema Einwilligung war in der Projektgruppe lange Zeit besonders streitig. Um neue Impulse für die projektgruppeninterne Diskussion zu erhalten, sollte die Öffentlichkeit dazu gezielt befragt werden. Im Forum auf der Microsite der Enquete-Kommission[374] konnten vom 20. Dezember 2010 bis 9. Januar 2011 Meinungen und Anregungen zu den folgenden fünf Punkten geäußert werden:

[371] Vgl. Wissenschaftliche Dienste des Deutschen Bundestages Becher, Johannes: Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedstaaten. 2011. WD 7 – 3000 – 036/11.

[372] Das Sondervotum schließt inhaltlich an das Ende des von der Enquete-Kommission verabschiedeten Textes zu Kapitel 3 an.

[373] BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 – Vorratsdatenspeicherung.

[374] https://www.bundestag.de/internetenquete/index.jsp

1. Voraussetzungen der Einwilligung

Welche Voraussetzungen sollten nach Ihrer Meinung für eine wirksame Einwilligung in die Erhebung und Verarbeitung personenbezogener Daten gegeben sein, und in welcher Form? Inwieweit ist für die Einwilligung zu differenzieren, z. B. nach der Art der jeweils betroffenen Daten oder nach dem jeweiligen Zweck der Datenverarbeitung? […]

2. Information und Transparenz

Welche Informationen müssen für Sie vorliegen, damit Sie eigenverantwortlich entscheiden können, ob und in welchem Umfang Sie Ihre Daten zur Verfügung stellen? […]

3. Grenzen der Freiwilligkeit und „ faktische Zwänge"

Welchen Stellenwert haben „ faktische Zwänge", einen bestimmten Dienst (z. B. soziale Netzwerke), zu nutzen und deshalb auch in die jeweilige Datenerhebung und -verarbeitung einzuwilligen? […]

4. Einwilligung und Widerspruch

Wie bewerten Sie die Möglichkeit, die Einwilligung in bestimmten Fällen durch einen von Ihnen zu erhebenden Widerspruch zu ersetzen (opt-in und opt-out)? […]

5. Praktische Ansätze

Wie sieht aus Ihrer Sicht eine Einwilligung aus, die einfach und praktikabel ist und Ihnen die Ausübung Ihres Rechts auf informationelle Selbstbestimmung ermöglicht? […][375]

Am Ende dieser Konsultationsphase lagen insgesamt 63 Antworten vor. Im Thread „Information und Transparenz" wurden die meisten Antworten geschrieben (18). Die wenigsten Antworten (6) gingen im Thread „Praktische Ansätze" ein.

Die Projektgruppe hat sich in ihrer Sitzung am 17. Januar 2011 ausführlich mit den Kommentaren und Ideen der Bürgerinnen und Bürger auseinandergesetzt. Viele der geäußerten Gesichtspunkte finden sich in den Texten der Projektgruppe wieder, wenn auch möglicherweise mit anderen Schlussfolgerungen. Beispielsweise wurde von mehreren Nutzern auf die Bedeutung der Transparenz hingewiesen. Zu dieser Frage hat sich die Projektgruppe in ihrem Bericht unter 2.1.2 *Grundprinzipien des Datenschutzrechts – Transparenzgrundsatz* und unter 2.3.2 *Ausgestaltung und Reichweite von Transparenzinstrumenten* ausführlich geäußert. Die von Nutzern mehrfach angesprochene Problematik der begrenzten Anwendbarkeit und Durchsetzbarkeit nationaler Datenschutzregelungen ist Gegenstand des Kapitels 2.1.9 *Die Grenzen des nationalen Datenschutzes.*

Da die Projektgruppe Datenschutz, Persönlichkeitsrechte eine der ersten Projektgruppen der Enquete-Kommission Internet und digitale Gesellschaft war, standen in den ersten Monaten ihrer Tätigkeit Beteiligungsmöglichkeiten aus technischen Gründen noch nicht in vollem Umfang zur Verfügung. Auch die Befragung der Bürgerinnen und Bürger zum Thema Einwilligung wurde zu einem Zeitpunkt durchgeführt, an dem außer dem Forum auf der Microsite der Enquete-Kommission andere Beteiligungstools noch nicht genutzt werden konnten.

5.2 Bürgerbeteiligung auf der Online-Beteiligungsplattform der Enquete-Kommission

Nachdem am 24. Februar 2011 die Online-Beteiligungsplattform der Enquete-Kommission[376] freigeschaltet worden war, hat die Projektgruppe Datenschutz, Persönlichkeitsrechte die Öffentlichkeit im Rahmen von zwei weiteren Beteiligungsphasen in ihre Arbeit einbezogen. Beginnend am 15. März 2011 wurden dort alle Texte, die von der Projektgruppe erarbeitet worden waren, zur Diskussion und Kommentierung eingestellt. Dies waren 61 Texte der Kapitel 1. *Bestandsaufnahme bestehender Datenschutzregelungen,* 2.1 *Datenschutz – Prinzipien, Ziele, Werte* und 2.2 *Datenschutz im öffentlichen Bereich* und 2.3 *Datenschutz im nicht-öffentlichen Bereich.* Entsprechend dem Fortgang der Arbeiten in der Projektgruppe wurden die Texte fortlaufend ergänzt. Bis zum 30. März 2011 konnten Texte bearbeitet und nachfolgend bis zum 4. April 2011 über Vorschläge abgestimmt werden.

Die Resonanz auf diese Papiere war gering. Dies ist möglicherweise darauf zurückzuführen, dass – bedingt durch den Zeitpunkt der Freischaltung der Online-Beteiligungsplattform – ein Einstieg in die Beteiligung erst erfolgen konnte, als die Arbeiten der Projektgruppe schon weit fortgeschritten waren. Eine kontinuierliche Beteiligung der Bürger durch alle Phasen der Projektgruppenarbeit war daher nicht mehr möglich.

Dass es auch anders geht, zeigte sich im Verlauf der zweiten Beteiligungsphase. Wesentliches Ziel der Enquete-Kommission Internet und digitale Gesellschaft ist es, politische Handlungsempfehlungen zu erarbeiten, die der weiteren Verbesserung der Rahmenbedingungen der Informationsgesellschaft in Deutschland dienen.[377] Daher war es wichtig, gerade bei der Formulierung der Handlungsempfehlungen, die sozusagen das Herzstück der Projektgruppenarbeit sind, Bürgerbeteiligung zu ermöglichen. Um eine erleichterte Beteiligung zu gewährleisten, wurde in dieser Beteiligungsphase auf die systemseitig eigentlich vorgesehene formalisierte Abstimmung verzichtet. Stattdessen erfolgte die Abstimmung über die Bewertungsmöglichkeit direkt am Vorschlag selbst.

[375] Zum vollständigen Wortlaut der Fragen siehe: Deutscher Bundestag. Enquete-Kommission Internet und digitale Gesellschaft. Diskussionsforum. https://forum.bundestag.de/forumdisplay.php?22-Fragen-der-Projektgruppe-Datenschutz-Pers%F6nlichkeitsrechte&s=56665542d 673002b7588eb0752606b8a

[376] https://enquetebeteiligung.de/

[377] Vgl. Beschluss zur Einsetzung einer Enquete-Kommission Internet und digitale Gesellschaft, Bundestagsdrucksache17/950, S. 4.

Zwischen dem 20. April 2011 und dem 17. Mai 2011 konnten entsprechende Vorschläge eingestellt werden. Die Ergebnisse wurden in den Projektgruppensitzungen am 9. Mai, 27. Mai und 6. Juni 2011 diskutiert.

Insgesamt haben sich 119 Online-Mitglieder für die Projektgruppe Datenschutz und Persönlichkeitsrechte der Beteiligungsplattform registriert und 32 Vorschläge[378] sowie 73 Kommentare abgegeben.[379] Davon wiesen 25 Vorschläge einen – häufig sehr direkten – inhaltlichen Bezug zu Problemstellungen auf, die von der Projektgruppe bei der Erarbeitung der Handlungsempfehlungen diskutiert worden waren, wie zum Beispiel die Vorschläge „Selbstdatenschutz fördern“ und „Schutz unseres Wohnungs-Nutzungsverhaltens im Zeitalter elektronischer Zähler“. Vier Vorschläge betrafen Fragen, die in der Projektgruppe bisher nicht erörtert worden waren. Dies gilt etwa für die Forderung, § 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) aufzuheben, oder für das Modell eines „Fair Trade“ von Daten im Internet. Drei Vorschläge beinhalteten nicht spezifisch datenschutzrechtliche Fragen.

In einigen Fällen deckten sich die Vorschläge der Bürgerinnen und Bürger vollständig oder zumindest sehr weitgehend mit Vorschlägen, die aus den Reihen der Projektgruppenmitglieder in die Diskussion eingebracht worden waren. Dies betrifft etwa die Empfehlungen, ein Verwertungsverbot für rechtswidrig erteilte Auskünfte über Nutzer von Internetdiensten einzuführen und erteilte Einwilligungen grundsätzlich zu befristen, sowie die Vorschläge, bei Datenschutzverstößen eine verschuldensunabhängige Ersatzpflicht auch für nicht-öffentliche Stellen und eine pauschalierte Entschädigung immaterieller Schäden vorzusehen.

In anderen Fällen haben sich Mitglieder der Projektgruppe Vorschläge aus der Online-Beteiligungsplattform der Enquete-Kommission zu Eigen gemacht und in ihre Texte übernommen. Diese Punkte sind also ausschließlich durch die Mitarbeit der Bürgerinnen und Bürger in die Projektgruppe hineingetragen worden. So sind die Forderung, dass im Hinblick auf die Einführung von IPv6 bei jedem Einwahlvorgang die dynamische Zuteilung einer neuen IP-Adresse anzubieten sei, und der Vorschlag „Systematische Evaluierung aller Überwachungsgesetze“ aus der Beteiligungsplattform in die Handlungsempfehlungen einzelner Fraktionen übernommen worden.[380]

Insgesamt hat sich gezeigt, dass die große Mehrzahl der Themen, die für die teilnehmenden Nutzerinnen und Nutzer wichtig waren, auch in den sonstigen Berichtsteilen der Projektgruppe Datenschutz, Persönlichkeitsrechte (das heißt insbesondere im Kapitel 2) aufgegriffen und erörtert wurden.

[378] Zwei dieser Vorschläge stammten bereits aus der ersten Beteiligungsphase (15. März bis 4. April 2011).
[379] Stand: 30. Juni 2011.
[380] Vgl. Kapitel 4.2.2 unter „Datenschutz auf technischer Ebene (Deep Packet Inspection und IPv6)“ sowie „Sicherheitsbehörden und die Evaluierung von Eingriffsbefugnissen“.

6 Literatur- und Quellenverzeichnis

6.1 Publikationen

Albers, Marion: Umgang mit personenbezogenen Daten und Informationen, in: Schmidt-Aßmann, Wolfgang (Hrsg.). Grundlagen des Verwaltungsrechts, Band II (§ 22). München: Verlag C. H. Beck 2008.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin: Datenschutzrecht – Kommentar. Stuttgart [u. a.] : Boorberg, Stand April 2010.

Birk, Dominik/Wegener, Christoph: Über den Wolken: Cloud Computing im Überblick. Datenschutz und Datensicherheit (DuD), 34 (2010) 641–645.

Bull, Hans Peter: Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen. Neue Verwaltungszeitschrift (NVwZ) 2011, 257–263.

Calliess, Christian/Ruffert, Matthias (Hrsg.): EUV/EGV – Das Verfassungsrecht der Europäischen Union mit europäischer Grundrechtecharta. Kommentar. München: Verlag C. H. Beck, 3. Auflage 2007.

Däubler, Wolfgang/u. a. (Hrsg.): Bundesdatenschutzgesetz, Kommentar. Frankfurt am Main: Bund Verlag GmbH, 3. Auflage 2010.

Ennulat, Mark: Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und -einrichtungen. Frankfurt am Main: Peter Lang GmbH, 2008.

Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus: EUV/AEUV. München: Verlag C. H. Beck, 5. Auflage 2010.

Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.): Beck'scher TKG-Kommentar. München: Verlag C. H. Beck, 3. Auflage 2006.

Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. München : Beck, C. H., 2003.

Gola, Peter/Schomerus, Rudolf: Bundesdatenschutzgesetz : BDSG – Kommentar. München: Verlag C. H. Beck, 10. Auflage 2010.

Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. Neue Juristische Wochenschrift (NJW), 63 (2010) 1035–1042.

Heidrich, Jörg/Wegener, Christoph. Sichere Datenwolken – Cloud Computing und Datenschutz. Multimedia und Recht (MMR), 13 (2009) 803–807.

Hinz, Christian: Onlinedurchsuchungen. Juristische Ausbildung (JURA), 31 (2009) 141–146.

Hoeren, Thomas: Das Telemediengesetz. Neue Juristische Wochenschrift (NJW), 60 (2007) 801–806.

Jarass, Hans Dieter: Charta der Grundrechte der Europäischen Union. Kommentar. München: Verlag C. H. Beck, 2010.

Kilian, Wolfgang/Heussen, Benno (Hrsg.): Computerrechts-Handbuch. München: Beck, 28. Ergänzungslieferung 2010.

Kloepfer, Michael/Schärdel, Florian: Grundrechte für die Informationsgesellschaft – Datenschutz und Informationszugangsfreiheit ins Grundgesetz? JuristenZeitung (JZ), 64 (2009) 453–462.

Kokott, Juliane/Sobotta, Christoph: Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrags von Lissabon. Europäische Grundrechtezeitschrift (EuGRZ), 37 (2010) 265–271.

Kölble, Josef (Hrsg.): Das Deutsche Bundesrecht – Systematische Sammlung der Gesetze und Verordnungen mit Erläuterungen. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, Hauptband 1949.

Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung – Aufgabe des Rechts? Die Verwaltung: Zeitschrift für Verwaltungswissenschaft, 40 (2007) 153–172.

Kühling, Jürgen/Bohnen, Simon: Zur Zukunft des Datenschutzrechts – Nach der Reform ist vor der Reform. JuristenZeitung (JZ), 65 (2010) 600–610.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. Frankfurt a. M. : Verlag Recht und Wirtschaft, 2008.

Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.): EU-Verträge. Wien: Linde Verlag, 5. Auflage 2010.

Maunz, Theodor/Dürig, Günter: Grundgesetz. München: Verlag C.H. Beck, 57. und 58. Ergänzungslieferung 2010.

Mayer-Schönberger, Viktor: Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press, 2009.

Meyer-Ladewig, Jens: Europäische Menschenrechtskonvention : Handkommentar. Baden-Baden : Nomos [u. a.], 3. Auflage 2011.

Petersen, Christin: Einheitlicher Ansprechpartner und Datenschutz. Landes- und Kommunalverwaltung, 20 (2010) 344–349.

Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2009.

Roßnagel, Alexander: Anmerkung zu EuGH Urt. v. 6. November 2003, C-101/01, Slg. 2003, I-12971 Rn. 87 – Lindqvist. Multimedia und Recht (MMR) 2004, 95–100.

Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. Multimedia und Recht (MMR), 2005, 71–75.

Sachs, Michael (Hrsg.): Grundgesetz: Kommentar. München: Beck, 5. Auflage 2009.

Schaar, Peter: Privacy by Design. Identity in the Information Society, 2 (2010) 267–274.

Scheuing, Dieter H.: Zur Grundrechtsbindung der EU-Mitgliedstaaten. Europarecht (EuR), 40 (2005) 162–192.

Schoch, Friedrich: Das Recht auf informationelle Selbstbestimmung. Juristische Ausbildung (JURA), 30 (2008) 352–359.

Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung. Multimedia und Recht (MMR), 13 (2010) 75–80.

Schulz, Wolfgang: Verfassungsrechtlicher „Datenschutzauftrag“ in der Informationsgesellschaft. Die Verwaltung, 32 (1999) 137–177.

Schwarze, Jürgen (Hrsg.): EU-Kommentar. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2. Auflage 2009.

Simitis, Spiros (Hrsg.): Kommentar zum Bundesdatenschutzgesetz. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 5. Auflage 2003.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 6. Auflage 2006.

Tinnefeld, Marie-Theres/Rauhofer, Judith: Whistleblower: Verantwortungsbewusste Mitarbeiter oder Denunzianten? Fragen an Grundrechte, Ethikrichtlinien und Arbeitsrecht. Datenschutz und Datensicherheit (DuD), 32 (2008) 717–723.

Weichert, Thilo: Cloud Computing und Datenschutz. Datenschutz und Datensicherheit (DuD), 34 (2010) 679-687.

Wolff, Heinrich A.: Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung? Neue Zeitschrift für Verwaltungsrecht (NVwZ), 29 (2010) 751–753.

Yildirim, Nuriye: Datenschutz im Electronic Government. Wiesbaden : Deutscher Universitäts-Verlag, 2004.

6.2 Online-Quellen (zuletzt aufgerufen am 23. Januar 2012)

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) vom 26./27. November 2009: Datenschutzkonforme Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten. http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) am 28./29. April 2010 (überarbeitete Fassung vom 23. August 2010): Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen. http://www.bfdi.bund.de/cae/servlet/contentblob/1103868/publicationFile/88848/290410_SafeHarbor.pdf

Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“). https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/index.php

Bundesamt für Sicherheit in der Informationstechnik. Essoh, Alexander Didier: Cloud Computing und Sicherheit – Geht denn das? Vortragspräsentation vom 19. November 2011. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/4GS_Tag/07_essoh_bsi.pdf?__blob=publicationFile

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: Pflicht des österreichischen Rundfunks zur namentlichen Mitteilung der Arbeitnehmerjahresbezüge ab einer bestimmtem Grenze an den Rechnungshof zur Aufnahme in einen öffentlichen Bericht („ORF“) (EuGH). Stellungnahme zum Urteil des Europäischen Gerichtshofs (EuGH) vom 20. Mai 2003, Az.: C-465/00, C-138/01, C-139/01. http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/Arbeit/Artikel/200503_OesterreichischerRundfunk.html?nn=408918

Bundesministerium für Wirtschaft und Technologie (Hrsg.): IKT-Strategie der Bundesregierung „Deutschland Digital 2015“. Strategiepapier von November 2010. http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM): Datenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht. Juni 2010. http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM): Datenschutzkodex für Geodatendienste – Entwurf. Dezember 2010. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/rote_linie_kodex.pdf?__blob=publicationFile

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM): Jugend 2.0, Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen. Studie von 2011. http://www.bitkom.org/files/documents/BITKOM_Studie_Jugend_2.0.pdf

De Maizière, Thomas: 14 Thesen zu den Grundlagen für eine gemeinsame Netzpolitik der Zukunft. Thesenpapier vom 22. Juni 2010. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/thesen_netzpolitik.pdf?__blob=publicationFile

Deutscher Bundestag. Enquete-Kommission Internet und digitale Gesellschaft: Diskussionsforum. https://forum.bundestag.de/forumdisplay.php?22-Fragen-der-Projektgruppe-Datenschutz-Pers%F6nlichkeitsrechte&s=56665542d673002b7588eb0752606b8a

Deutscher Bundestag. Enquete-Kommission für Internet und digitale Gesellschaft: Zwischenbericht Medienkompetenz. Bundestagsdrucksache 17/7286 vom 21. Oktober 2011. http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Medienkompetenz_1707286.pdf

Grimme Online Award: Zur Begründung der Jury bezüglich des Preisträgers 2011. http://www.grimme-institut.de/html/index.php?id=1345

Hickey, Hannah: This article will self-destruct: A tool to make online personal data vanish. University of Washington vom 21. Juli 2009. http://www.washington.edu/news/archive/id/50973

Hinrichs, Lars: Schriftliche Stellungnahme im Rahmen der Öffentlichen Anhörung „Auswirkungen der Digitalisierung auf unsere Gesellschaft – Bestandsaufnahme, Zukunftsaussichten“ der Enquete-Kommission Internet und Digitale Gesellschaft des Deutschen Bundestages am 5. Juli 2010. A.-Drs. 17(24)004-D. http://www.bundestag.de/internetenquete/dokumentation/2010/Sitzungen/20100705/A-Drs__17_24_004-D_-_Stellungnahme_Hinrichs.pdf

Institut für Demoskopie Allensbach im Auftrag der SCHUFA Holding AG: Die Einstellung der Deutschen zum Thema Datenschutz. Studie von September 2010. Pressemitteilung unter: http://www.schufa.de/de/private/presse/aktuellepressemitteilungen/2010/100929.jsp

Klein, A./Leithold, Franziska/Zell, Christine/Roosen, Jutta: Digitale Profilbildung und Gefahren für die Verbraucher. TU München, Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes e. V. von November 2010. http://www.vzbv.de/mediapics/digitale_profilbildung_tu_muenchen_leithold_2010.pdf

Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010. http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile

Landesbeauftragter für den Datenschutz Niedersachsen. Herausforderungen für den Datenschutz bei eGovernment. http://www.lfd.niedersachsen.de/live/live.php?navigation_id=13010&article_id=56234&_psmand=48

Matzat, Lorenz: Malte Spitz’ Vorratsdaten: Der Datensatz unter der Lupe. ZEIT ONLINE vom 24. Februar 2011. http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/

Online-Beteiligungsplattform der Enquete-Kommission. https://enquetebeteiligung.de/

Rosen, Jeffrey: The Web means the End of Forgetting. The New York Times vom 21. Juli 2010. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern. 2002. www.computerundrecht.de/media/gutachten.pdf

Sirix AG security technologies im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik. Ergänzende und alternative Techniken zu Trusted Computing (TC-Erg./-A.), Teil 1. Version vom 29. Januar 2010. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/TC_ErgA/TC-ErgA_Teil1.pdf

Sokol, Bettina: Neunzehnter Datenschutz- und Informationsfreiheitsberichts der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen für die Jahre 2007 und 2008, 2009. https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/19_DIB/DIB_2009.pdf

TNS Infratest im Auftrag von Microsoft: Studienergebnisse „Datenschutz im digitalen Zeitalter – Trends und Spannungsfelder“. Mai/Juni 2011. http://download.microsoft.com/download/2/0/B/20BE3B2A-7563-40C7-9BD6-9CF5E2AEF5ED/Datenschutzstudie_2011_Microsoft.pdf

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Bizer, Johann: eGovernment: Chance für den Datenschutz. 2005 https://www.datenschutzzentrum.de/e-government/dud-200507.htm

Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein. Weichert, Thilo: Cloud Computing und Datenschutz. Mai 2010. https://www.datenschutzzentrum.de/cloud-computing/

Universität des Saarlandes: X-pire! – Wie man dem Internet das „Vergessen“ beibringt. Stand: 2011. http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/

WELTONLINE: Spitzelaffäre kostet Lidl 1,5 Millionen Euro. Artikel vom vom 11. September 2008. http://www.welt.de/wirtschaft/article2428529/Spitzelaffaere-kostet-Lidl-1-5-Millionen-Euro.html

ZEIT ONLINE: Verräterisches Handy. Artikel vom 31. August 2009. http://www.zeit.de/datenschutz/maltespitz-vorratsdaten

7 Mitglieder der Projektgruppe Datenschutz, Persönlichkeitsrechte der Enquete-Kommission Internet und digitale Gesellschaft

Vorsitzender:	Manuel Höferlin (MdB, FDP)
Stellvertretender Vorsitzender:	Dr. Reinhard Brandl (MdB, CDU/CSU)
Wissenschaftliche Mitarbeiterin:	Antje Franz

Stimmberechtigt:

Brandl, Dr. Reinhard (MdB, CDU/CSU)

Höferlin, Manuel (MdB, FDP)

Jarzombek, Thomas (MdB, CDU/CSU)

Koeppen, Jens (MdB, CDU/CSU)

Notz, Dr. Konstantin von (MdB, BÜNDNIS 90/DIE GRÜNEN)

Rohleder, Dr. Bernhard (Sachverständiger)

Schröder, Lothar (Sachverständiger)

Tausch, Cornelia (Sachverständige)

Wawzyniak, Halina (MdB, DIE LINKE.)

weitere Mitglieder:

Beckedahl, Markus (Sachverständiger)

Brand, Michael (MdB, stellvertr. Mitglied der Enquete-Kommission, CDU/CSU)

Drobinski-Weiß, Elvira (MdB, stellvertr. Mitglied der Enquete-Kommission, SPD)

Freude, Alvar C. H. (Sachverständiger)

Gersdorf, Prof. Dr. Hubertus (Sachverständiger)

Hofmann, Jeanette (Sachverständige)

Klingbeil, Lars (MdB, SPD)

Knoerig, Axel (MdB, stellvertr. Mitglied der Enquete-Kommission, CDU/CSU)

Kurz, Constanze (Sachverständige)

Lemke, Harald (Sachverständiger)

Mayer, Stephan (MdB, stellvertr. Mitglied der Enquete-Kommission, CDU/CSU)

Montag, Jerzy (MdB, stellvertr. Mitglied der Enquete-Kommission, BÜNDNIS 90/DIE GRÜNEN)

Mühlberg, Annette (Sachverständige)

Osthaus, Dr. Wolf (Sachverständiger)

padeluun (Sachverständiger)

Puttrich, Lucia (MdB, stellvertr. Mitglied der Enquete-Kommission, CDU/CSU)[381]

Reichenbach, Gerold (MdB, SPD)

Rößner, Tabea (MdB, BÜNDNIS 90/DIE GRÜNEN)

Schwarzelühr-Sutter, Rita (MdB, stellvertr. Mitglied der Enquete-Kommission, SPD)

Thomae, Stephan (MdB, stellvertr. Mitglied der Enquete-Kommission, FDP)

[381] Aus dem Deutschen Bundestag ausgeschieden am 3. September 2010.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333